나무위키

I2P

최근 수정 시각: 2026-08-23 05:35:08

분류:프록시 | 파일 공유 | 다크 웹 | 프라이버시

목차

1. 개요
2. I2P EasyInstall Bundle
3. 토어 브라우저를 이용해서 I2P 사용하기
4. Hidden Mode
5. I2PSnark
6. I2PD
7. Syndie
8. I2P 삭제
9. 모네로
10. 억압적인 국가에서의 검열 우회
11. 같이 보기

- https://geti2p.net/ko/

1. 개요

I2P는 Tor와 비슷한 프록시 프로그램이다. 하지만 Tor와는 달리 외부 네트워크에 접속하는 기능보다는 흔히 다크 웹이라고 불리는 내부 네트워크 기능에 초점이 맞춰져 있다. 내부 네트워크 기능으로는 메일, IRC, 호스팅, 토렌트 등을 이용할 수 있다. 하지만 Hyphanet과 같이 지나치게 마이너한지라 범죄도 거의 없다시피 한다.

내부 네트워크만 사용하면 Tor보다 속도가 가끔씩은 느릴 때도 있지만 대체로 빠르다. 토렌트는 외부와의 통신이 불가능하지만 익명으로 공유가 가능하다. 하지만 Vuze를 이용하면 외부와 내부 전부 이용 가능하지만, 외부 토렌트를 이용하면 익명성이 깨진다. 또, 설정 페이지에 서비스가 모두 (영어지만) 소개되어 있어 이 점은 사용하기 편하다.

모든 사용자는 Tor의 relay와 같은 역할을 해야 한다. 그리고 설정, 설치 등이 복잡하기 때문에 진입 장벽이 Tor보다 살짝 더 높다. 게다가 안타깝게도 I2P는 한글로 번역이 되어 있지 않고 한글로 된 소개글, 사용 방법은 거의 없는 상황이다. 그리고 이것을 통해 외부 사이트 접근은 거의 불가능하다. Outproxy 부족 때문인데 Tor가 빠르게 느껴지니 말 다 했다.

'Ramble'이라는 I2P 커뮤니티 사이트에서 한국어 포럼을 찾아서 볼 수 있다.
한국 I2P Ramble 포럼 @

2. I2P EasyInstall Bundle

- 권장사항

I2P를 사용해 보기 전에 가상 사설망, Tor, Tails OS, Whonix 문서를 모두 정독한 뒤 I2P를 사용해 보는 것을 적극 권장한다.
해외 사이트인 Reddit의 I2P 서브레딧을 자주 눈팅하면 정보를 얻기 좋다.

I2P EasyInstall Bundle을 이용하여 I2P를 이용해 보자.

I2P EasyInstall Bundle 사용법

1. Firefox 다운.

2. I2P Easy Install Bundle 설치. 설치과정을 완료하고 잠깐 기다리면 I2P가 실행된다.

I2P for Windows

Download I2P for Windows

i2pinstall_2.3.0_windows.exe
Mirror: sigterm.no

select alternate mirror
sig

The default I2P installer requires Java to be installed. You can obtain it from Oracle or from your choice of Java distribution. After installing Java, download the file and double-click to run it.

Easy Install Bundle For Windows (Beta)

It is now possible to install all I2P components using a single package (**No Java required**). To try out the new installer, click below. This bundle can also be used to configure a Firefox Profile. It will not interfere with an existing I2P installation if one exists.

I2P Easy Install Bundle For Windows (Beta)

Detailed Install Guide

Here is a helpful guide to installing I2P for Windows using a separate Java installation and the classic installer.

How do I use it?

First, download and install Firefox, then, just download and install this installer(below). To start an installer, "double-click" the downloaded .exe file.

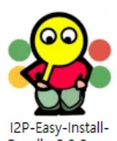
Running the installer will create a shortcut to start browsing I2P in your start menu and on your desktop. Clicking this shortcut will start I2P if necessary, then start an I2P Browser. On the first run, you will also be promted with the bandwidth wizard in your browser window. You will also see a "Toopie" icon in your taskbar to indicate that I2P is working when the browser window is closed.

I2P Browsing uses a separate, I2P-Only Firefox profile, so it won't interfere with your regular Firefox use or require any special configuration. You don't even need to close existing Firefox windows.

I2P-Easy-Install-Bundle-2.3.0.exe
Mirror: sigterm.no

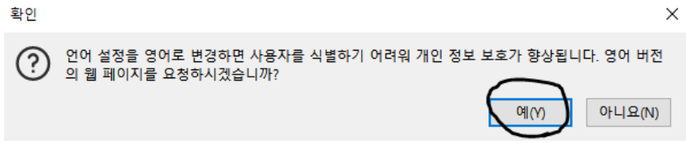
select alternate mirror

Download that file and complete the steps it shows.

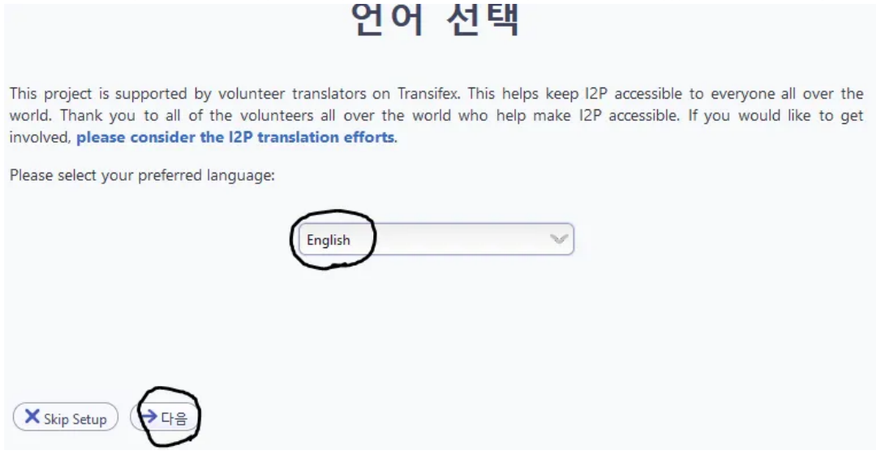


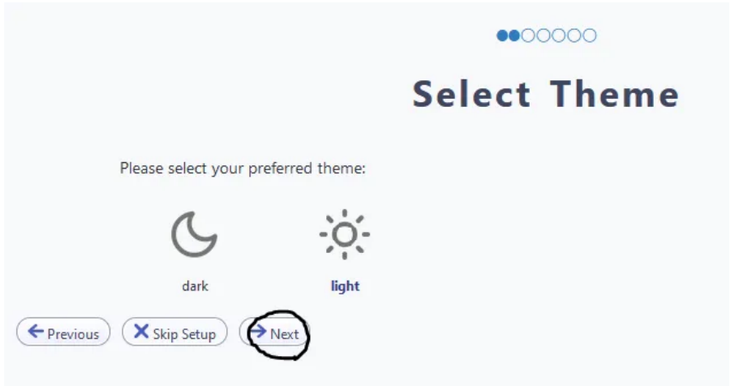
I2P-Easy-Install-Bundle-2.3.0.exe

3. 언어 설정을 영어로 변경.



4. I2P 설정 과정 진행. 언어를 영어로 바꿔준다. 그 뒤로는 잘 모르겠으면 Next만 누르면 된다.


언어 선택
This project is supported by volunteer translators on Transifex. This helps keep I2P accessible to everyone all over the world. Thank you to all of the volunteers all over the world who help make I2P accessible. If you would like to get involved, please consider the I2P translation efforts.
Please select your preferred language:
English
Skip Setup
다음



Bandwidth Test

Let's check your internet connection!

Bandwidth participation not only makes your speed and connection to the I2P network better, but also helps everyone using the network. When everyone is sharing as much bandwidth as possible, everyone gets to have better performance and privacy by sharing participating traffic.

I2P uses M-Lab, a third party service, to help you test your internet connection and find the optimal speed settings. During this time you will be connected directly to M-Lab's service with your real IP address.

Please review the M-Lab privacy policies linked below. If you do not wish to run the M-Lab bandwidth test, you can skip it and configure your bandwidth later.

M-Lab Privacy Policy
M-Lab Name Server Privacy Policy

Previous | Skip Setup | Skip Bandwidth Test | Next

Bandwidth Test in Progress

Javascript is disabled - wait 60 seconds for the bandwidth test to complete and then click Next

While the I2P router software is getting ready to go, it's testing your bandwidth, obtaining an initial set of peers from a reseed server, making its first few connections, and getting integrated with the rest of the network.

To learn more about how important I2P Reseed servers are, or explore other topics and what functions they perform for I2P, you can visit the **I2P Wiki**. If you would like to discuss I2P topics or get help from the community, you can visit the **I2P Forums**. If you want to know more about the I2P Project itself, or the Invisible Internet in general, you can visit our **Project Website**.

Previous | Skip Setup | Cancel Bandwidth Test | Next

Bandwidth Configuration

I2P will work best if you configure your rates to match the speed of your internet connection.

8798	KBps In	(70.4 Mbits per second; 23.6 TBytes per month maximum)
36898	KBps Out	(295 Mbits per second; 98.8 TBytes per month maximum)
80%	Share	(56.3 Mbits per second; 18.85 TBytes per month maximum)

You have configured I2P to share 7,038 KBps.
By donating your bandwidth to participating traffic, you not only help others, you improve your own anonymity and performance.
We recommend sharing 75% or more for I2P, but you can adjust based on your needs.

Previous | Skip Setup | Next

Browser and Application Setup

Your browser needs to be configured to work with I2P. We have instructions for configuring both Firefox and Chromium based browsers with I2P. You can find these instructions on our **website**.

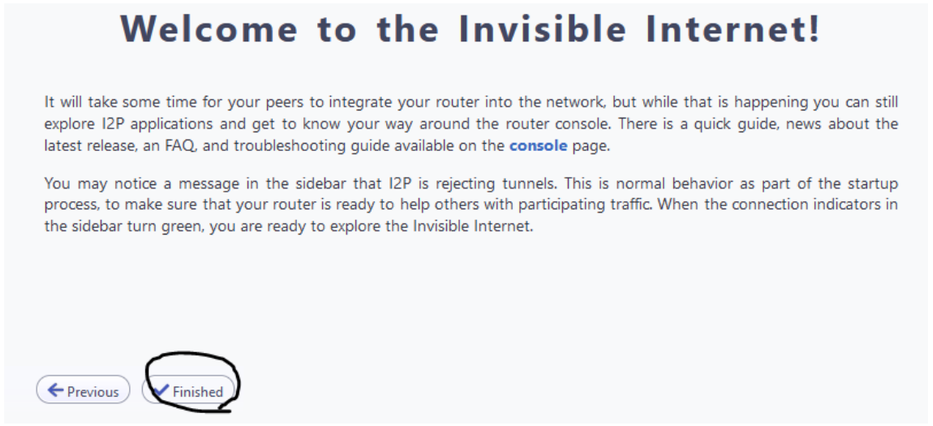
Otherwise, the recommended way to browse I2P websites is with a separate profile in the Firefox browser.

1. **Install Firefox**
2. **Install the I2P Firefox profile**

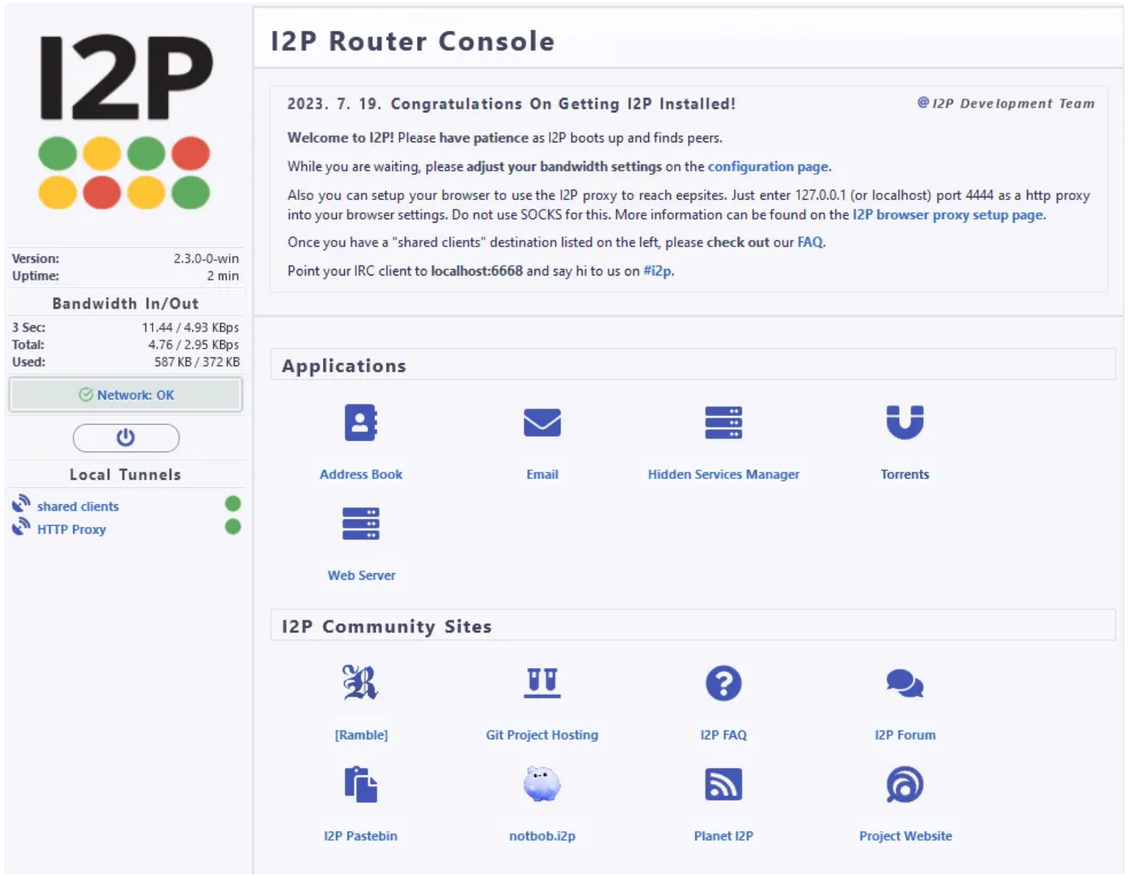
The I2P router also comes with its own versions of common, useful internet applications. You can download files with **bittorrent**. You can also send and receive **email**. Besides that, you can use the built-in **web server** so you can create, communicate, and share your content. These applications work with I2P automatically and require no additional configuration.

To help make I2P addresses easier to read and remember, the I2P router also includes its built-in **Address Book**. The Address Book is where you keep track of all your I2P "Contacts" by giving them human-readable names. This can be used for the sites you like to visit, messaging contacts, or potentially any other service on I2P. To help you get started, the address book can be used to subscribe to lists of addresses distributed by other I2P users.

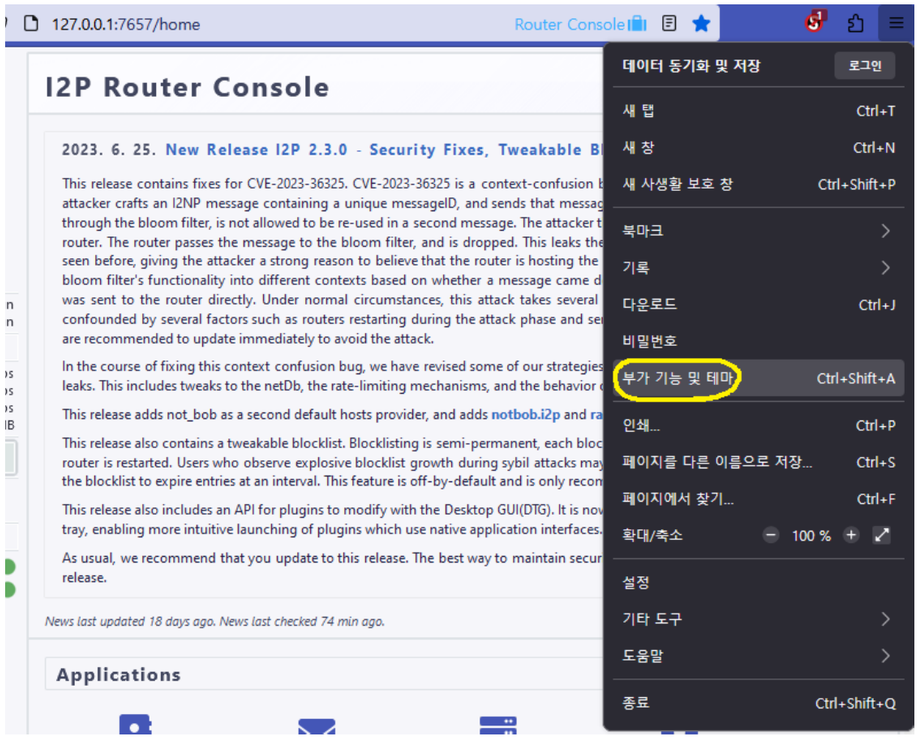
Previous | Skip Setup | Next

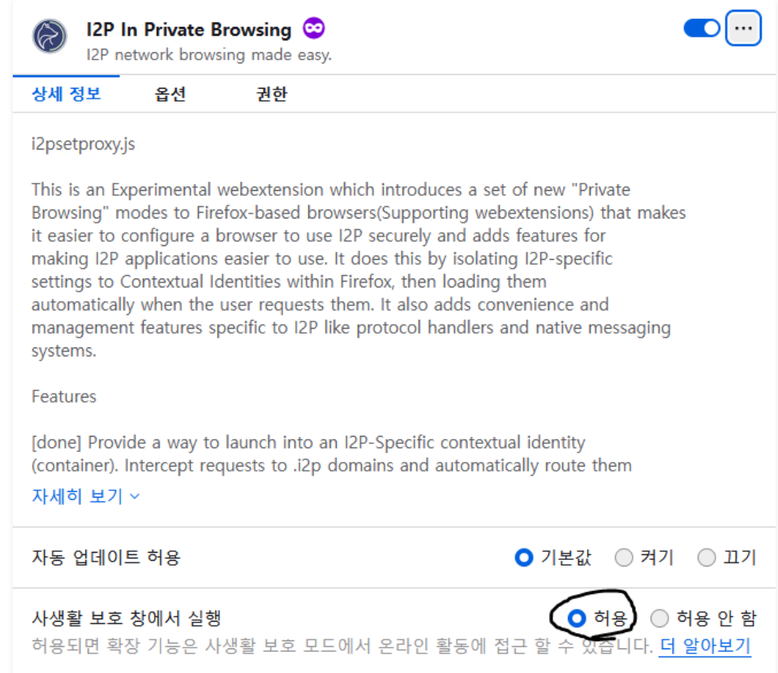


5. 메인 홈페이지의 모습이다.



6. 인터넷 기록을 남기고 싶지 않도록 시크릿 모드로 실행한다. 시크릿 모드에서도 확장프로그램이 실행되도록 설정한다.





NoScript

Maximum protection for your browser: NoScript allows active content only for trusted domains of your choice to prevent exploitation.

상세 정보 권한

Winner of the "PC World - World Class Award" and bundled with the Tor Browser, NoScript gives you the best available protection on the web. It allows JavaScript, Flash, and other executable content to run only from trusted domains of your choice (e.g. your banking site), thus mitigating remotely exploitable vulnerabilities, such as Spectre and Meltdown.

It protects your "trust boundaries" against cross-site scripting attacks (XSS), cross-zone DNS rebinding / CSRF attacks (router hacking), and Clickjacking attempts, thanks to its unique ClearClick technology.

Such a preemptive approach prevents exploitation of security vulnerabilities (known and unknown!) with no loss of functionality where you need it. Experts do agree: Firefox is really safer with NoScript ;-)

FAQ: https://noscript.net/faq
Forum: https://noscript.net/forum

자세히 보기

이 부가 기능의 개발자가 여러분이 작은 기여로 지속적인 개발을 지원해 줄 것을 요청합니다.

♥ 기여하기

자동 업데이트 허용 ◉ 기본값 ○ 켜기 ○ 끄기

사생활 보호 창에서 실행 ◉ 허용 ○ 허용 안 함

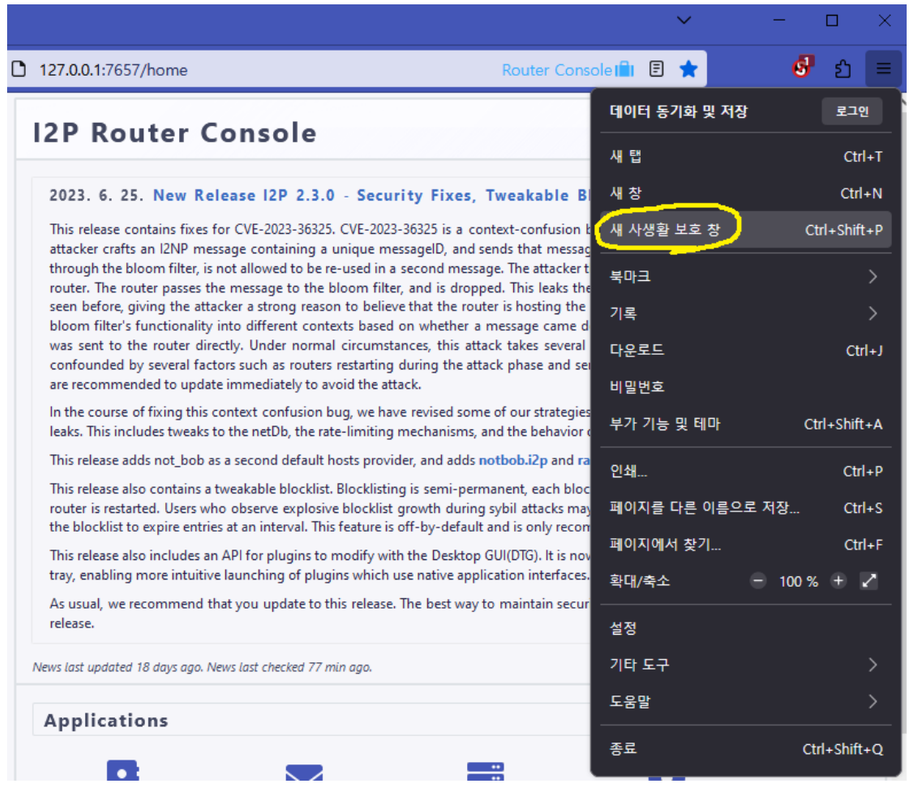
허용되면 확장 기능은 사생활 보호 모드에서 온라인 활동에 접근 할 수 있습니다. 더 알아보기

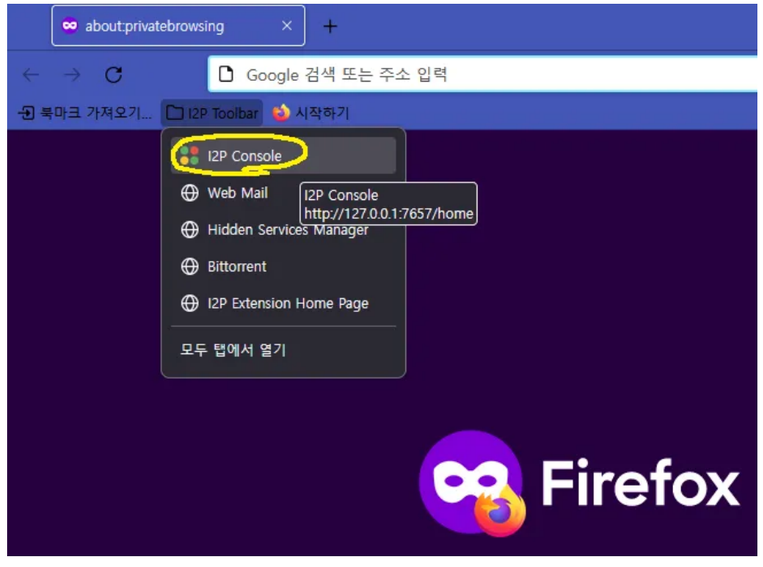
확장 기능 관리

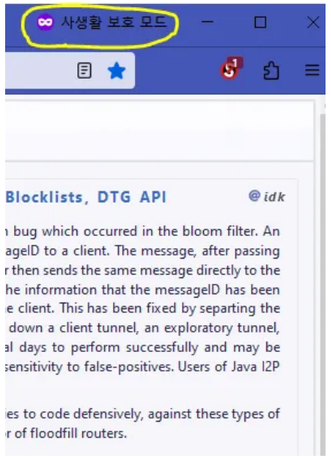
사용함

I2P In Private Browsing
I2P network browsing made easy.

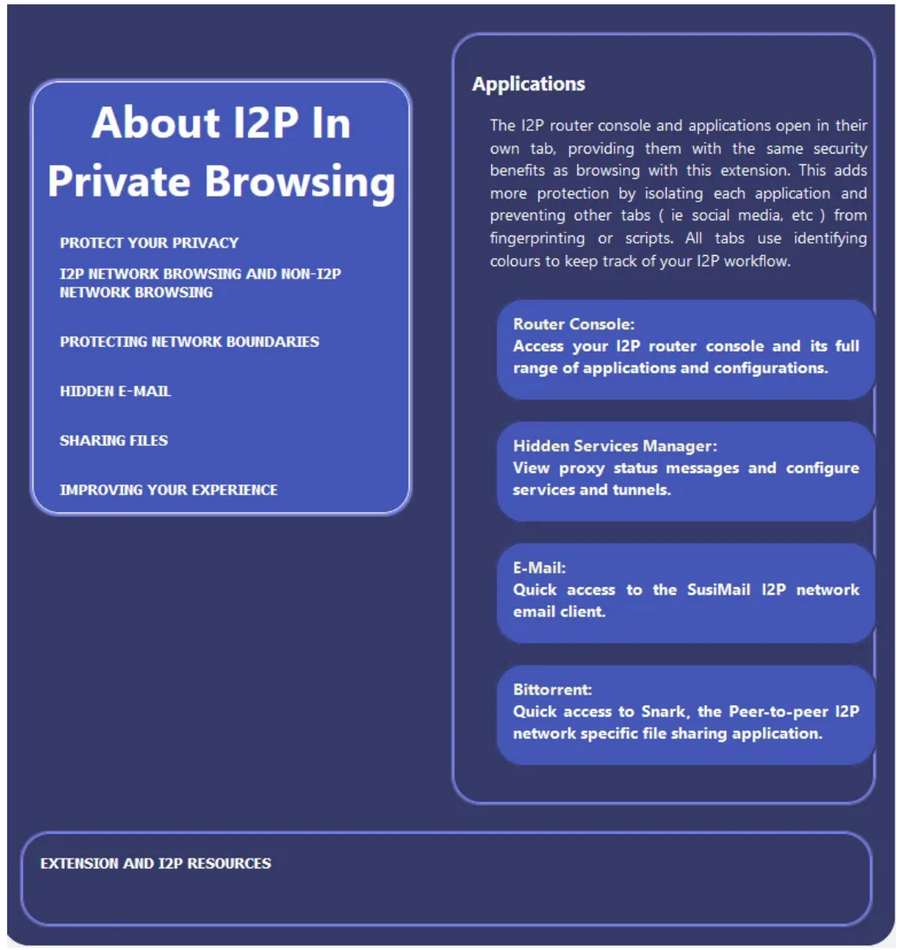
NoScript
Maximum protection for your browser: NoScript allows active content only for trusted do...

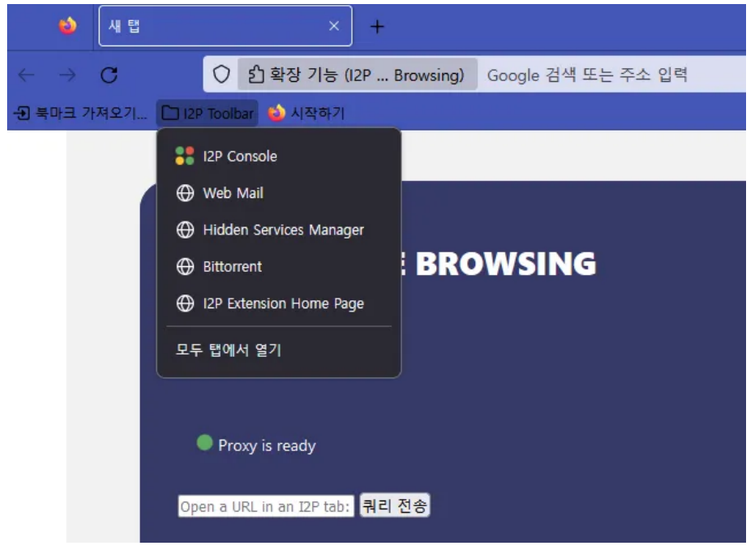




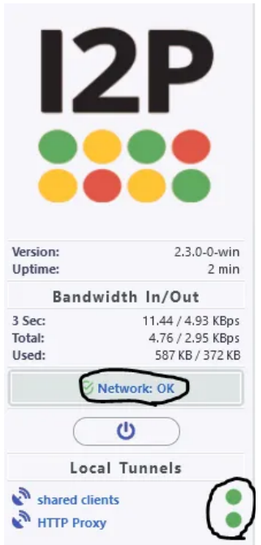


7. 새 탭을 열었을 때의 모습이다.

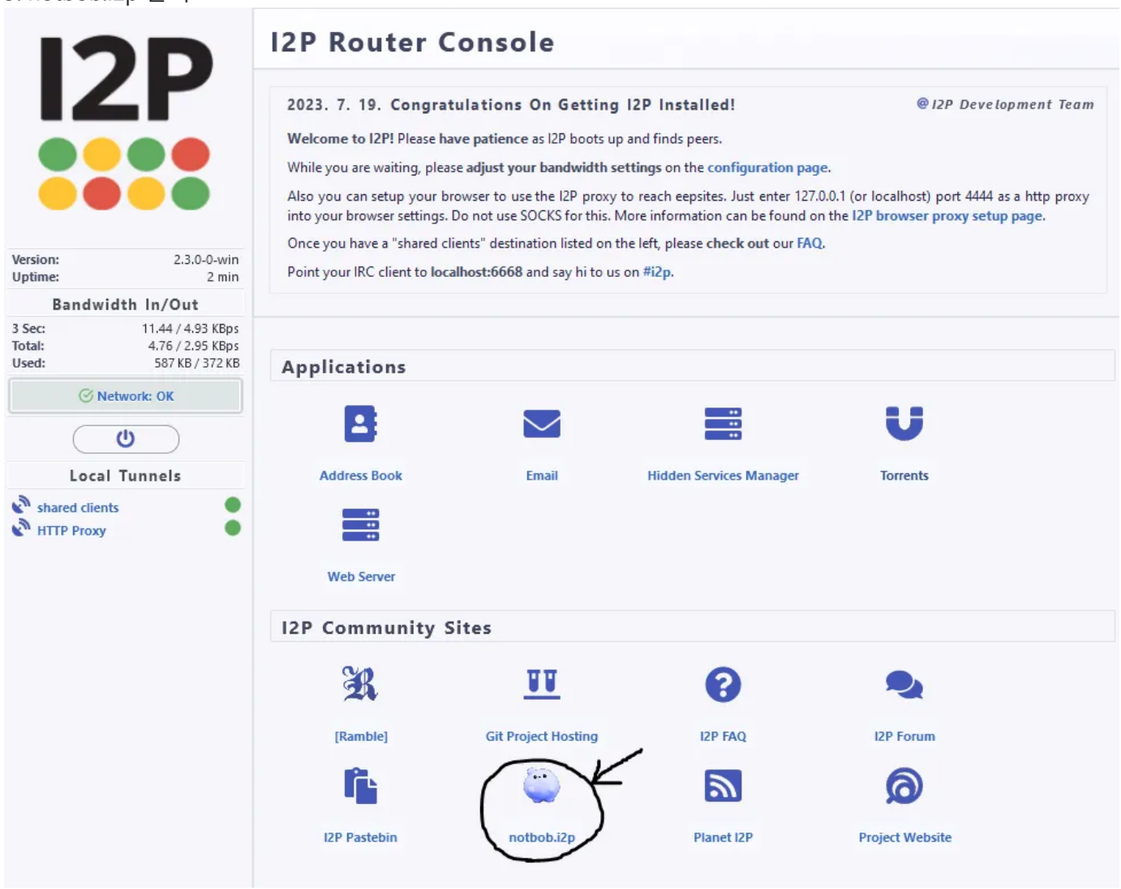




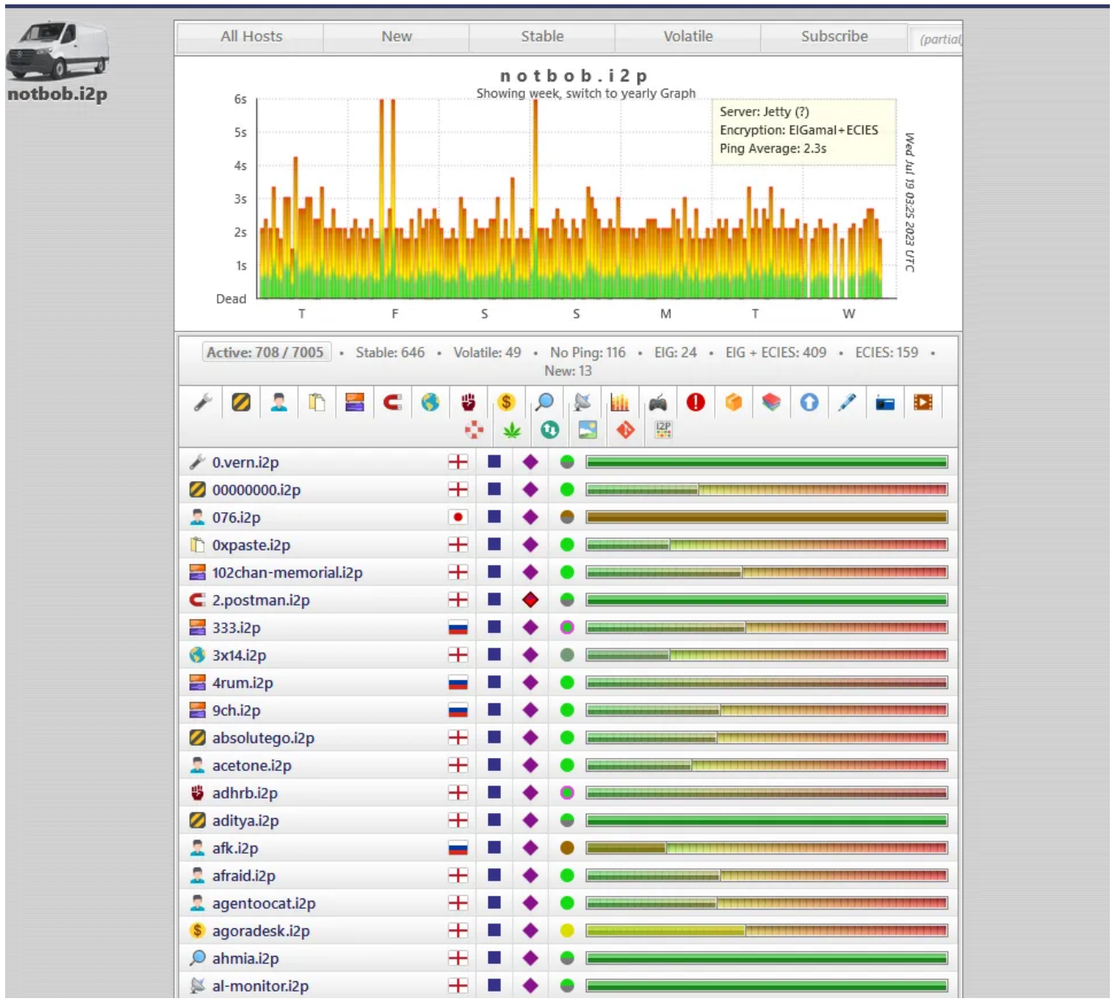
8. 연결이 잘되는지 확인한다.



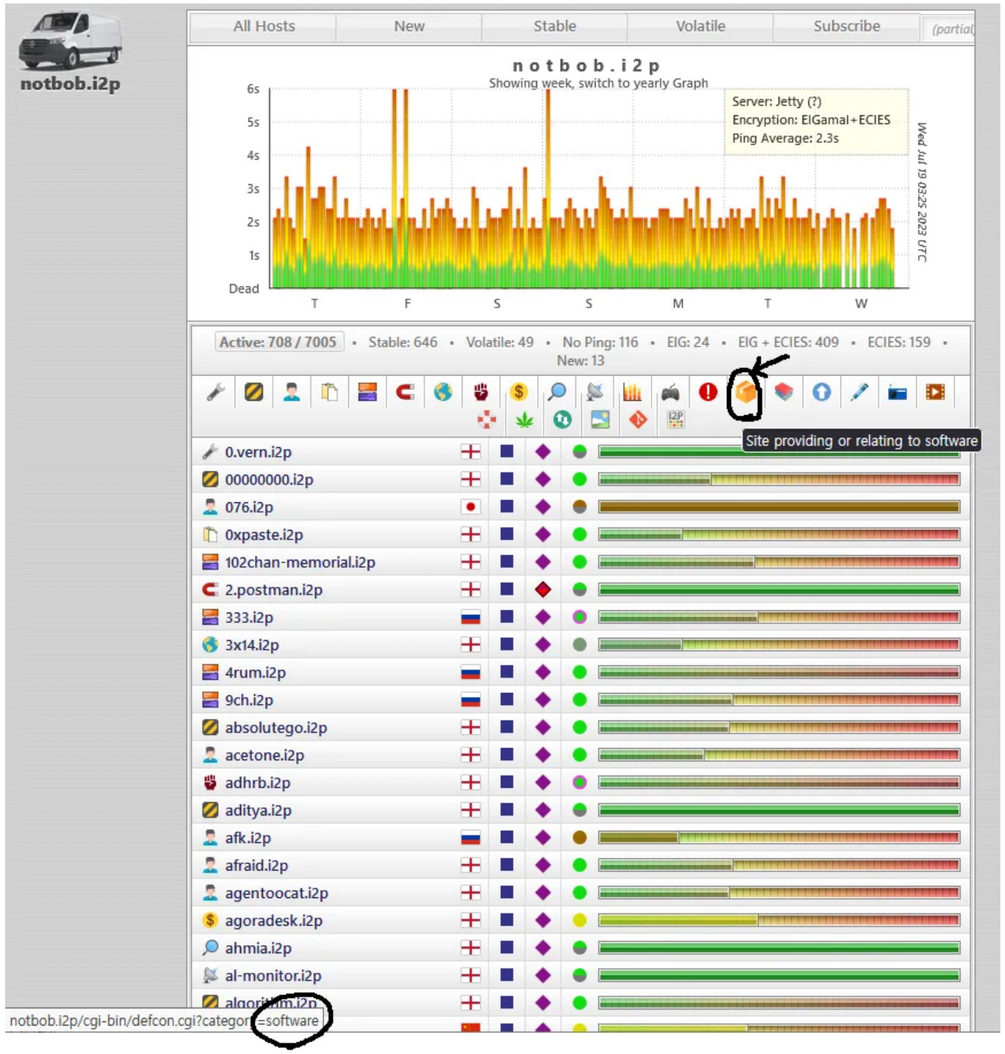
9. notbob.i2p 클릭


I2P Router Console
2023. 7. 19. Congratulations On Getting I2P Installed!
I2P Development Team
Welcome to I2P! Please have patience as I2P boots up and finds peers.
While you are waiting, please adjust your bandwidth settings on the configuration page.
Also you can setup your browser to use the I2P proxy to reach eepsites. Just enter 127.0.0.1 (or localhost) port 4444 as a http proxy into your browser settings. Do not use SOCKS for this. More information can be found on the I2P browser proxy setup page.
Once you have a "shared clients" destination listed on the left, please check out our FAQ.
Point your IRC client to localhost:6668 and say hi to us on #i2p.
Applications
Address Book
Email
Hidden Services Manager
Torrents
Web Server
I2P Community Sites
[Ramble]
Git Project Hosting
I2P FAQ
I2P Forum
I2P Pastebin
notbob.i2p
Planet I2P
Project Website

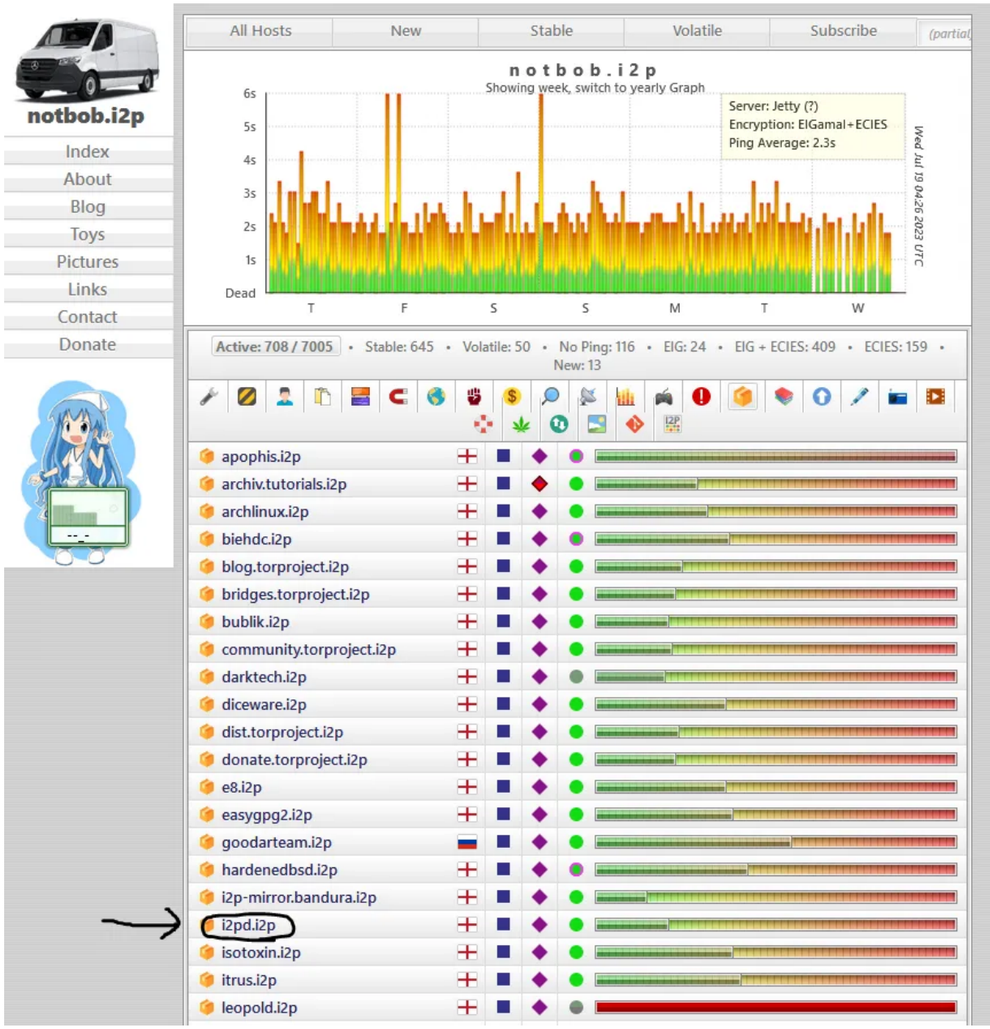
10. notbob.i2p 사이트의 전체적인 모습이다.



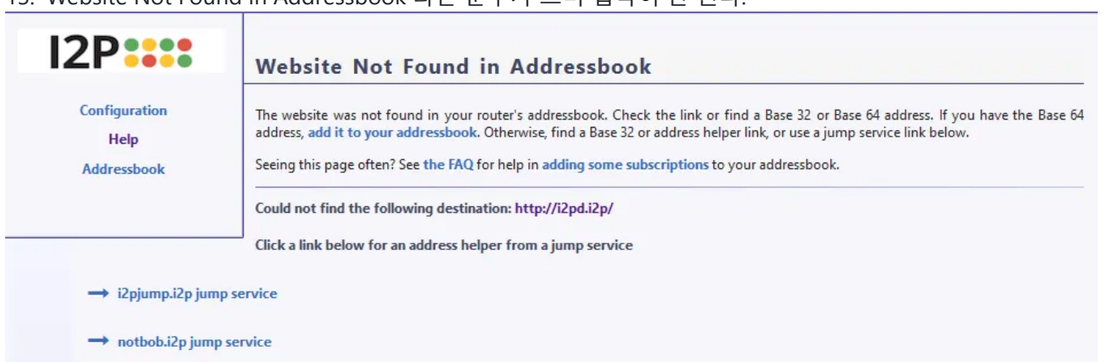
11. 박스모양 아이콘(Site providing or relating to software)을 클릭한다. 왼쪽 아래의 주소 문구로도 사이트 분류를 알 수 있다.



12. i2pd.i2p 클릭.

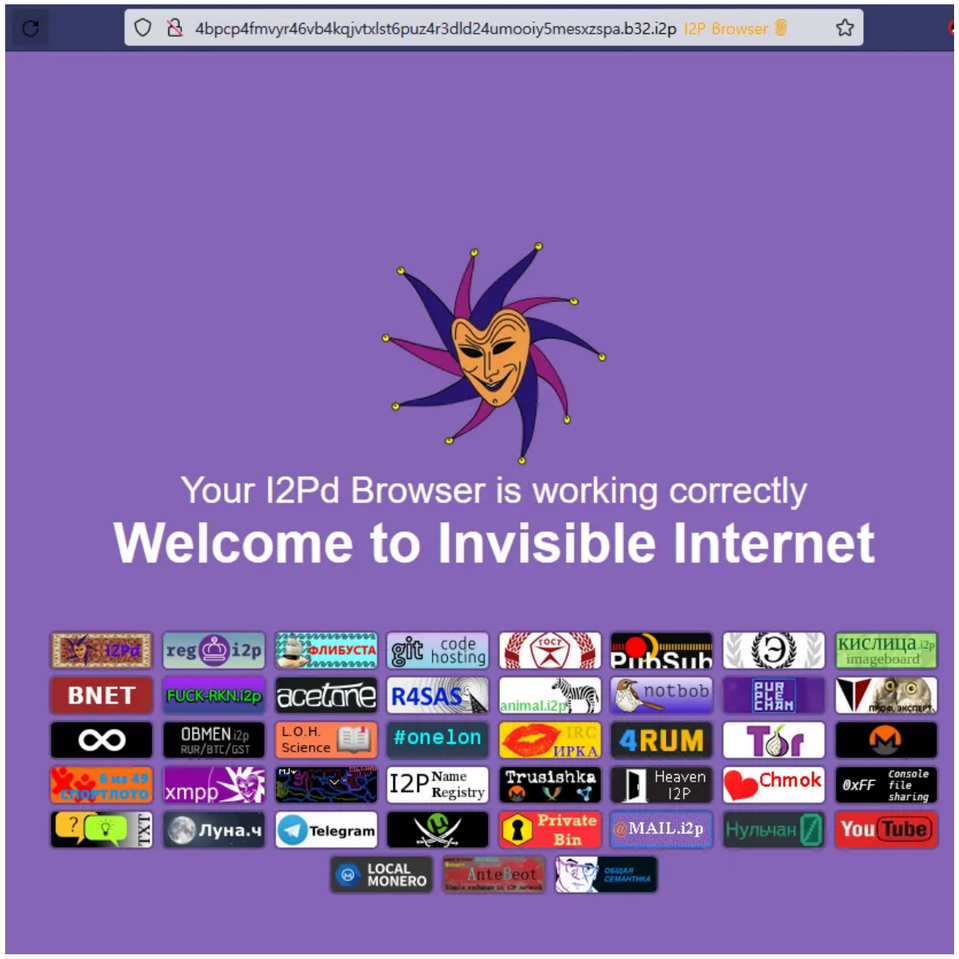


13. 'Website Not Found in Addressbook'라는 문구가 뜨며 접속이 안 된다.


I2P
Configuration
Help
Addressbook
Website Not Found in Addressbook
The website was not found in your router's addressbook. Check the link or find a Base 32 or Base 64 address. If you have the Base 64 address, add it to your addressbook. Otherwise, find a Base 32 or address helper link, or use a jump service link below.
Seeing this page often? See the FAQ for help in adding some subscriptions to your addressbook.
Could not find the following destination: http://i2pd.i2p/
Click a link below for an address helper from a jump service
i2pjump.i2p jump service
notbob.i2p jump service

14. 사이트 오른쪽의 사각형 아이콘(Base32 주소) 클릭.

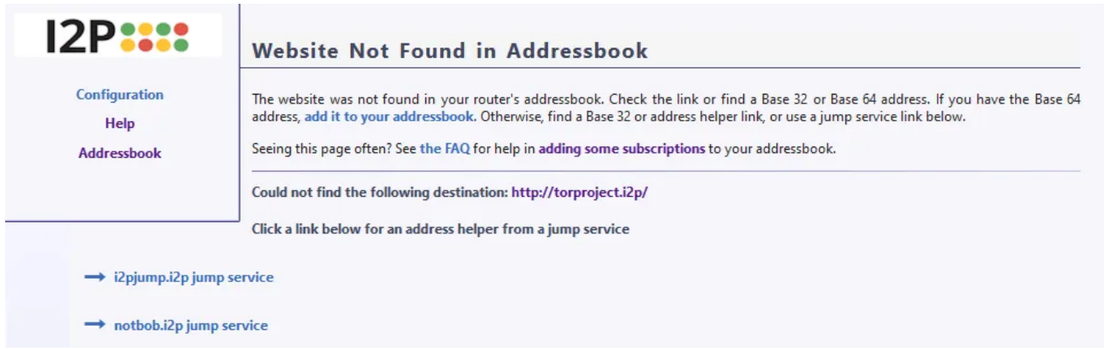
15. 사이트에 정상적으로 접속되었다. 해당 사이트는 🔗i2pd 브라우저를 실행했을 때 맨 처음 나오는 메인페이지이다.



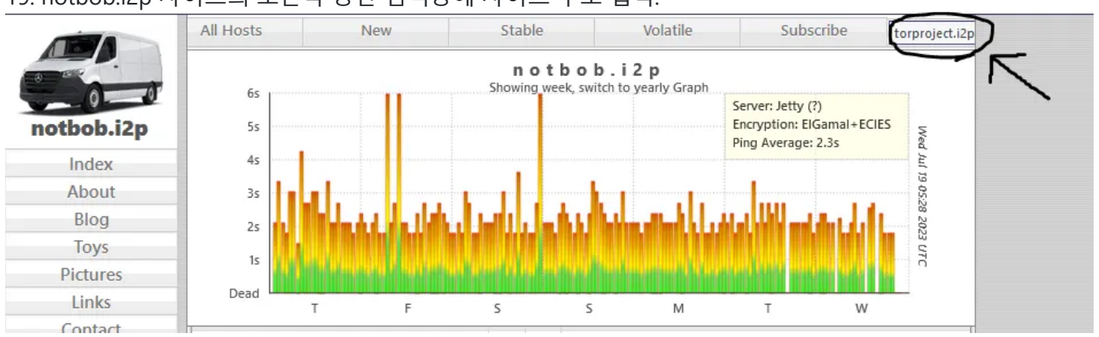
16. 만약 'Website Unreachable'라는 문구가 뜨며 접속이 안 된다면, 조금 기다렸다가 새로고침(F5) 몇 번 해보면 된다.

17. 한번 더 해보자. Tor 아이콘 클릭.

18. 이번에도 'Website Not Found in Addressbook'라는 문구가 뜨며 접속이 안 된다.

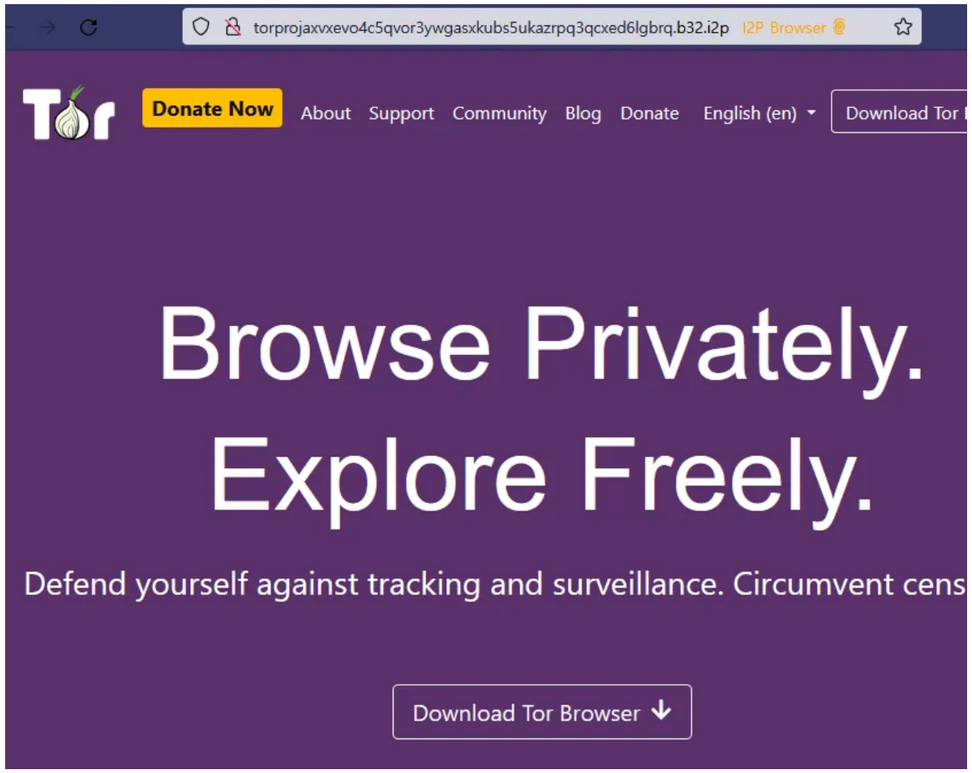


19. notbob.i2p 사이트의 오른쪽 상단 검색창에 사이트 주소 입력.



20. 사이트 오른쪽의 사각형 아이콘(Base32 주소) 클릭.

21. 사이트에 정상적으로 접속되었다.



지금까지 I2P Easy Bundle을 사용하는 방법을 알아보았다.

I2P Easy-install Bundle은 절대 익명이 아니다. 핑거프린팅 방어가 전혀 안 되기 때문이다. I2P Easy-install Bundle로 사이트를 탐방을 하는 것은 매우 위험하다. 그러므로 토어 브라우저를 세팅해서 I2P를 이용해야 한다.

3. 토어 브라우저를 이용해서 I2P 사용하기

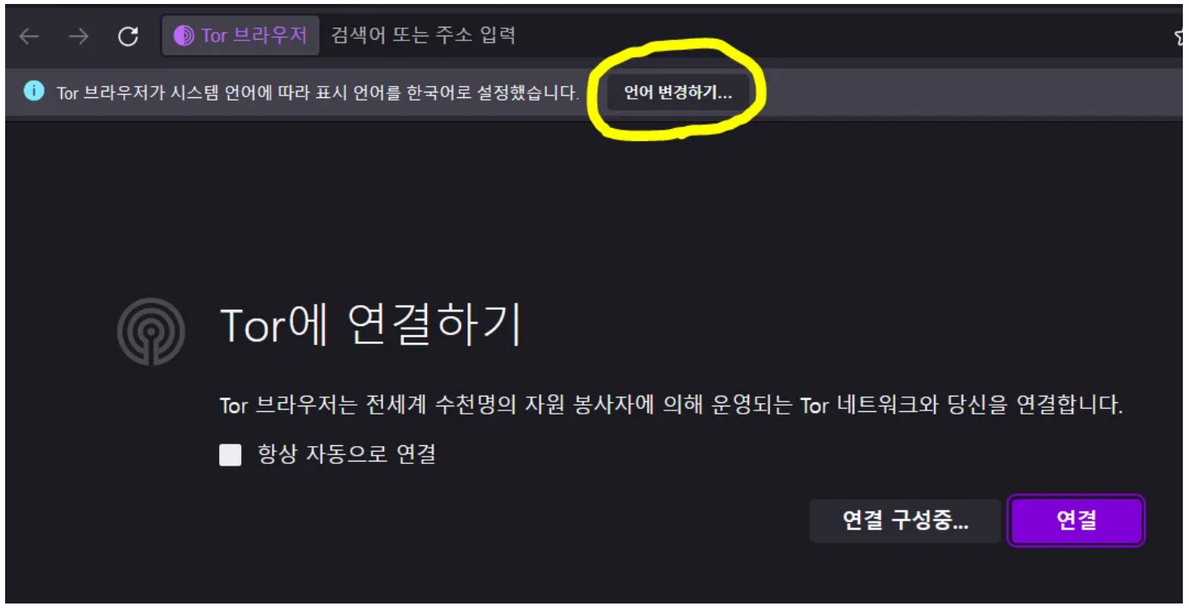
주의사항
1. 아래의 글은 토어 브라우저를 쓸 뿐 토어 네트워크는 쓰지 않는다.
2. 애초에 Windows는 프라이버시에 아주 나쁜 OS이다. 리눅스에서 I2P를 이용하는 것을 매우 권장한다.
3. Virtualbox 같은 가상머신을 이용하면 매우 좋다. 혹시라도 탐방하다가 악성코드에 감염되더라도 가상머신이 막아줄 수 있기 때문이다.
4. Whonix나 Qubes OS에서 I2P를 사용하는 것이 가장 안전하다. 참고로 Tails OS는 I2P 사용이 불가능하다.
5. 익명 네트워크 특성상 탐방하다가 불법 사이트를 발견할 수도 있는데 들어가지 않는 것을 적극 권장한다.

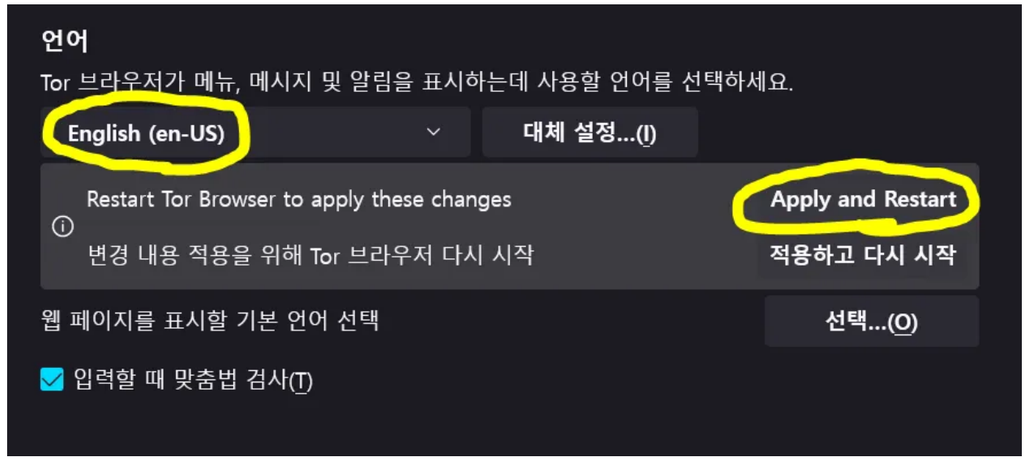
토어 브라우저를 세팅하여 I2P를 이용해 보자.

🔗 토어 브라우저를 이용해서 I2P 사용하는법

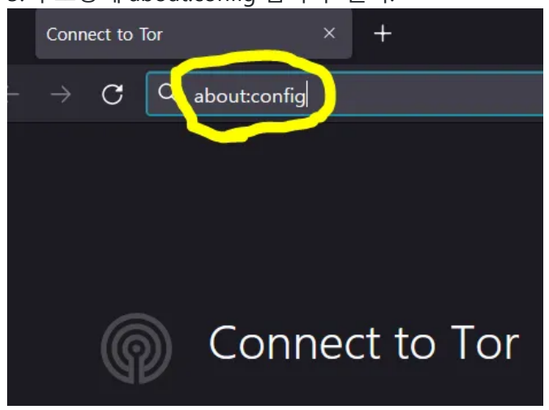
1. 🔗 I2P, 🔗 Java, 🔗 Tor Browser 다운로드.

2. 토어 브라우저 설치 후 언어를 영어로 변경한다.

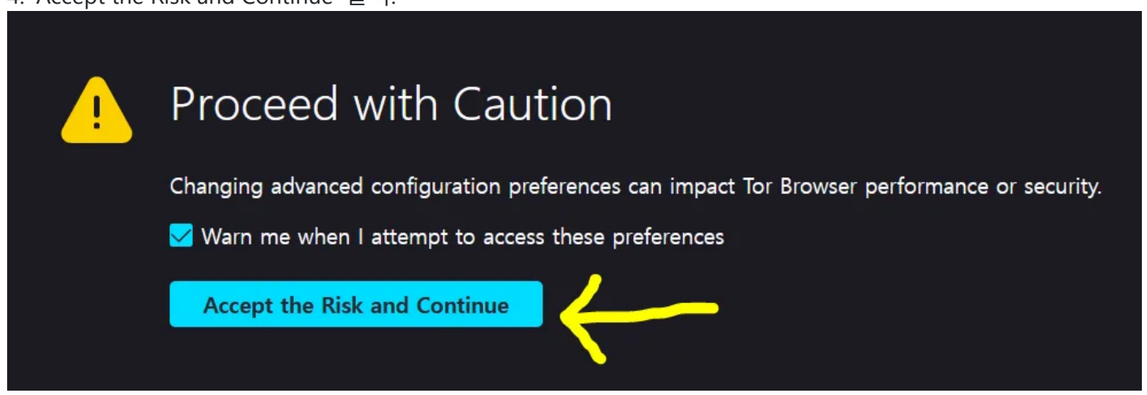




3. 주소창에 about:config 입력 후 엔터.



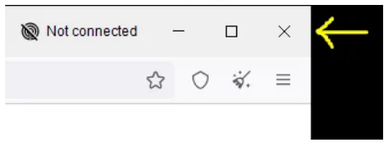
4. 'Accept the Risk and Continue' 클릭.


Proceed with Caution
Changing advanced configuration preferences can impact Tor Browser performance or security.
Warn me when I attempt to access these preferences
Accept the Risk and Continue

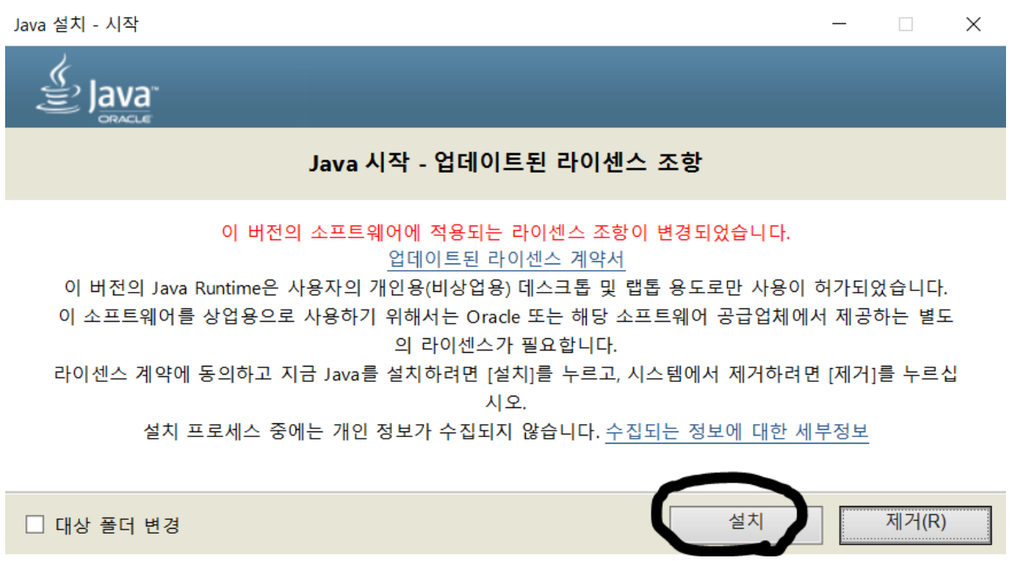
5. 아래와 같이 설정한다.
extensions.torbutton.use_nontor_proxy - true
network.proxy.http - 127.0.0.1
network.proxy.http_port - 4444
network.proxy.no_proxies_on - 127.0.0.1
dom.security.https_first_pbm - false
dom.security.https_only_mode - false
dom.security.https_only_mode_pbm - false
출처 - 🔗 https://www.whonix.org/wiki/I2P

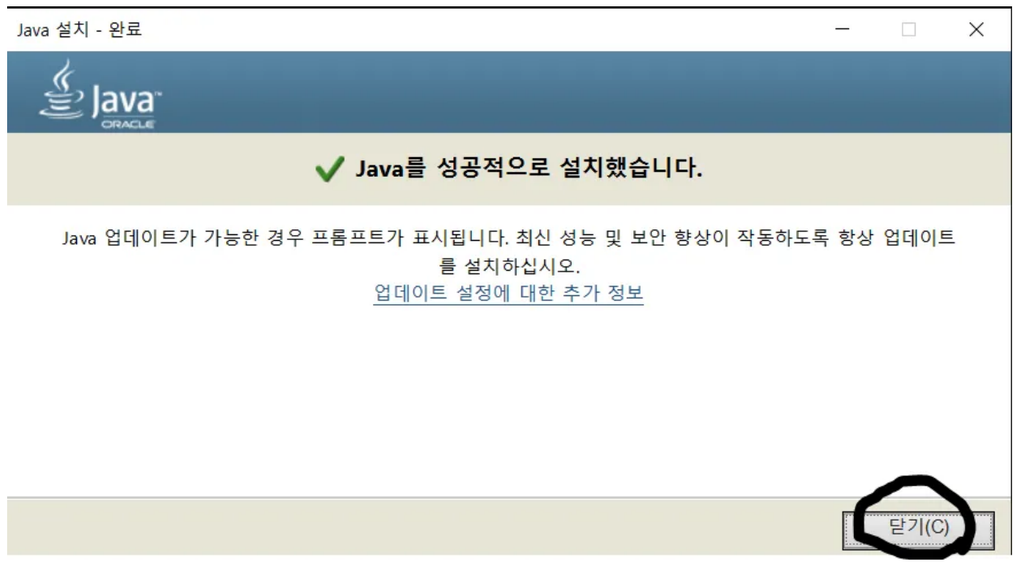
extensions.torbutton.use_nontor_proxy	true
network.proxy.http	127.0.0.1
network.proxy.http_port	4444
network.proxy.no_proxies_on	127.0.0.1
dom.security.https_first_pbm	false
dom.security.https_only_mode	false
dom.security.https_only_mode_pbm	false

6. 토어 브라우저 창 닫기.

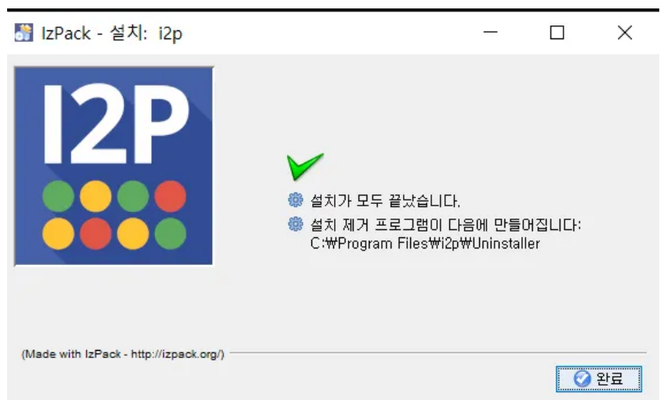


7. Java 설치.

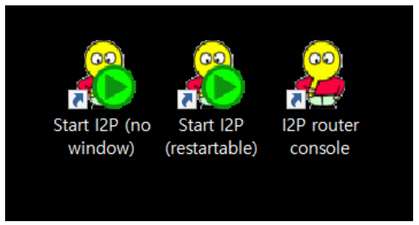




8. I2P 설치.

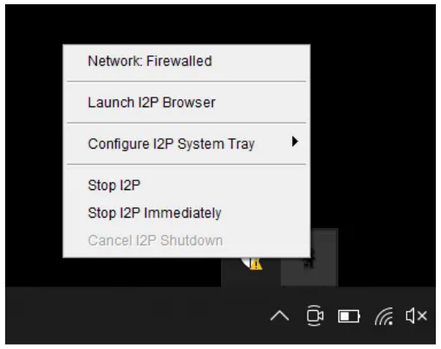


9. 바탕화면에 Start I2P(no window), Start I2P(restartable), I2P router console 3개의 아이콘이 생긴다.

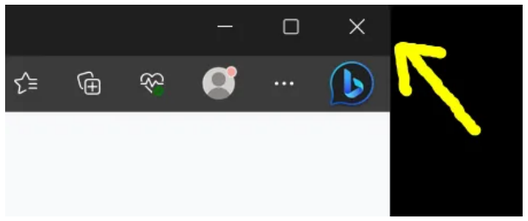


10. Start I2P(no window) 클릭.

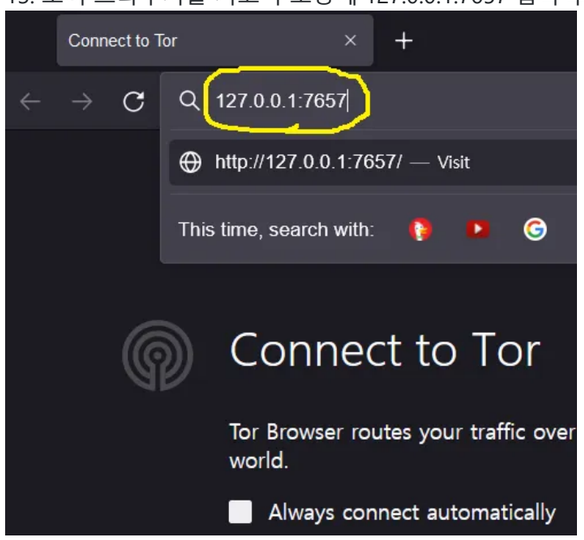
11. 바탕화면 오른쪽 아래에 아이콘이 생기는 것을 볼 수 있다.



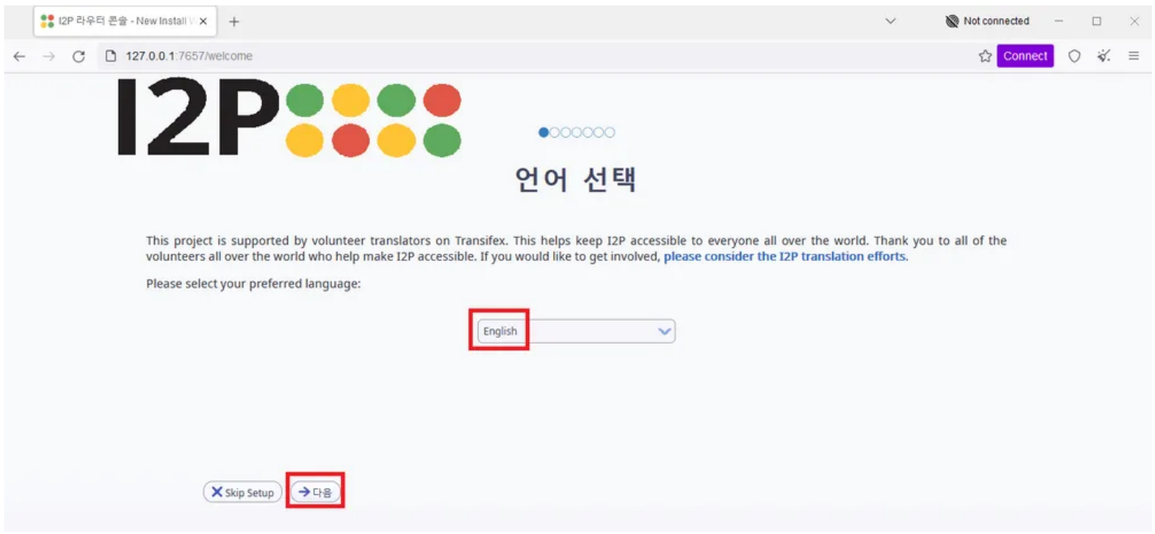
12. 엣지 브라우저가 실행되는 데 필요 없으므로 닫기.



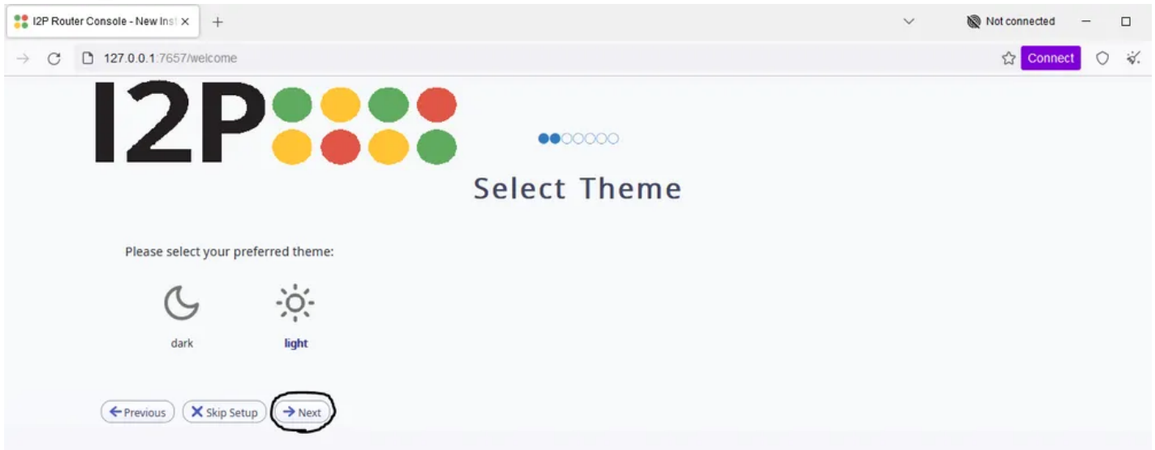
13. 토어 브라우저를 켜고 주소창에 127.0.0.1:7657 입력 후 엔터.



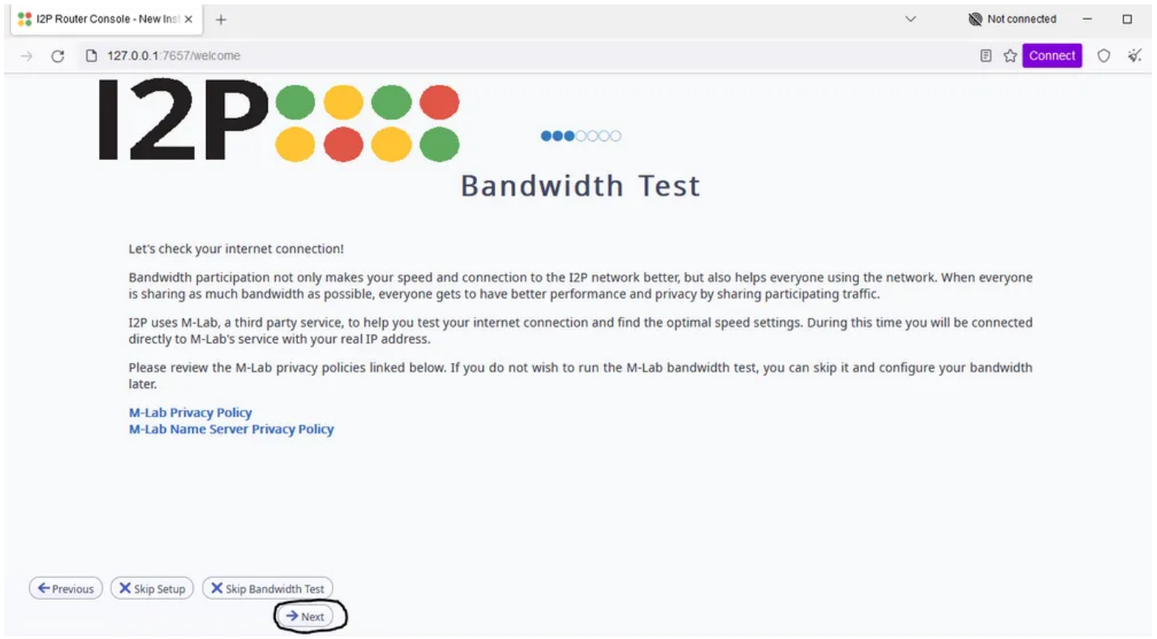
14. I2P 설정 과정 진행. 언어를 영어로 바꿔준 뒤 Next 클릭.



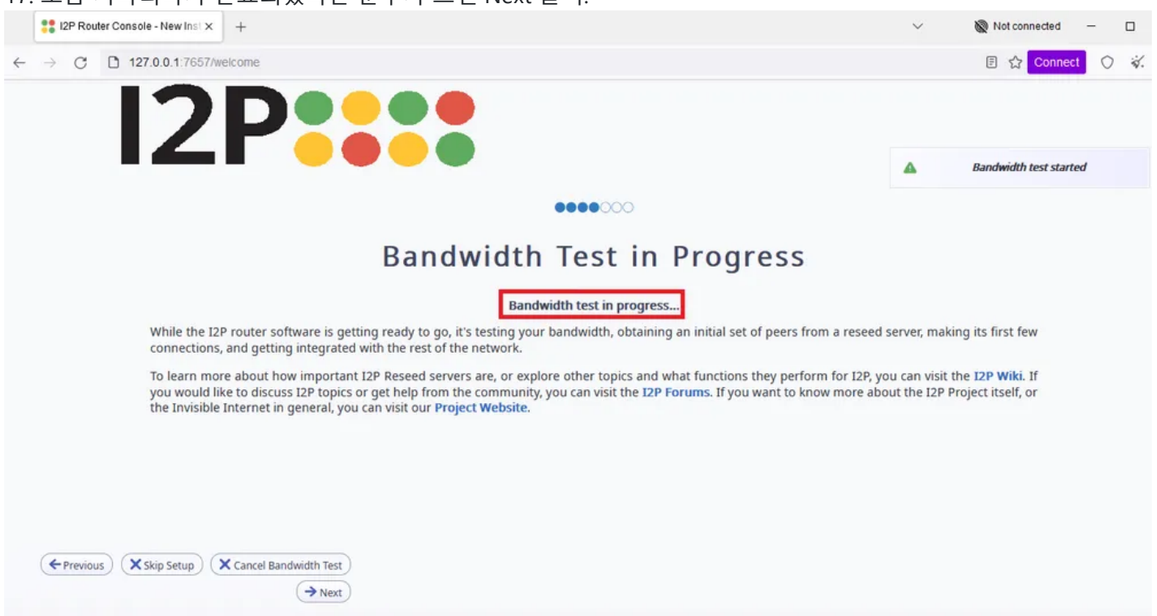
15. Next 클릭.



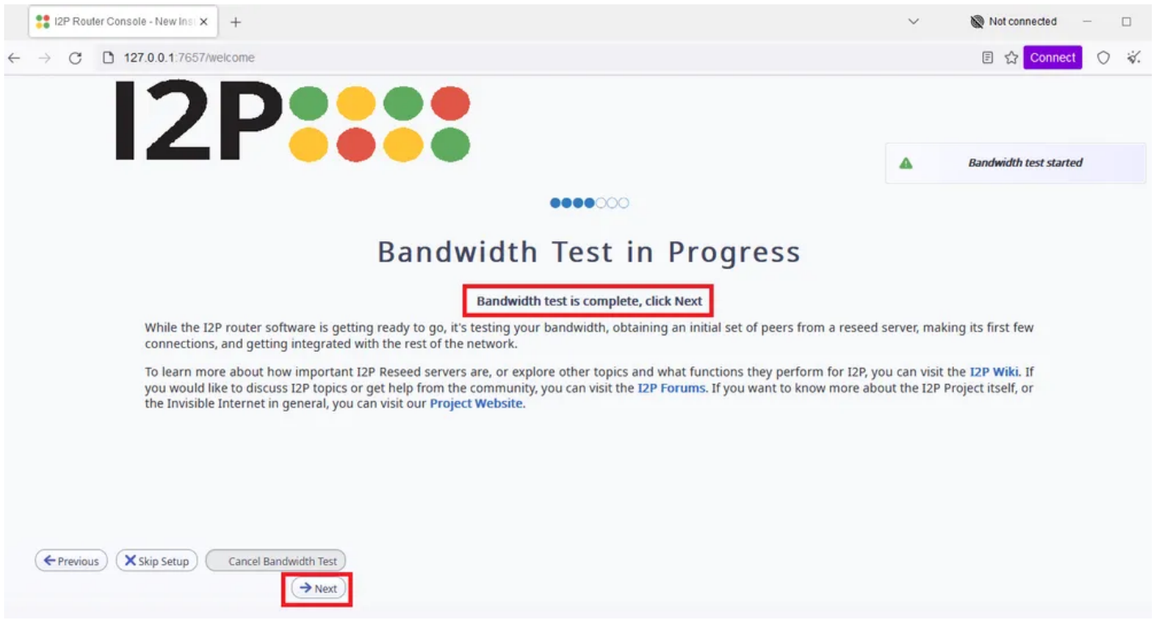
16. Next 클릭.



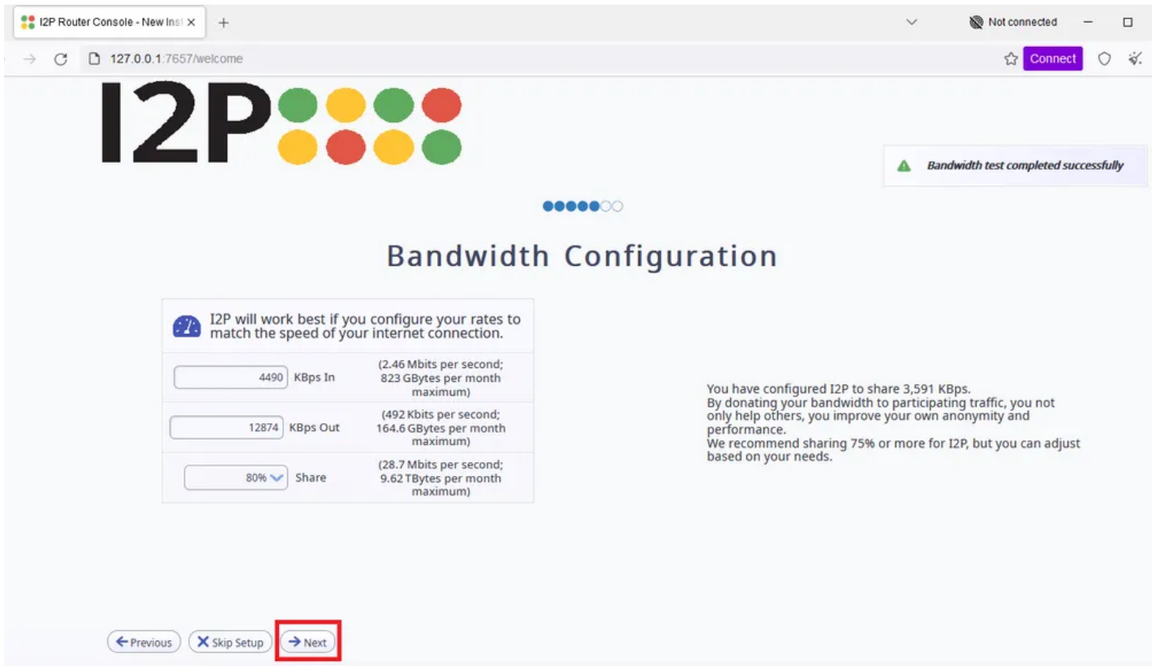
17. 조금 기다리다가 완료되었다는 문구가 뜨면 Next 클릭.

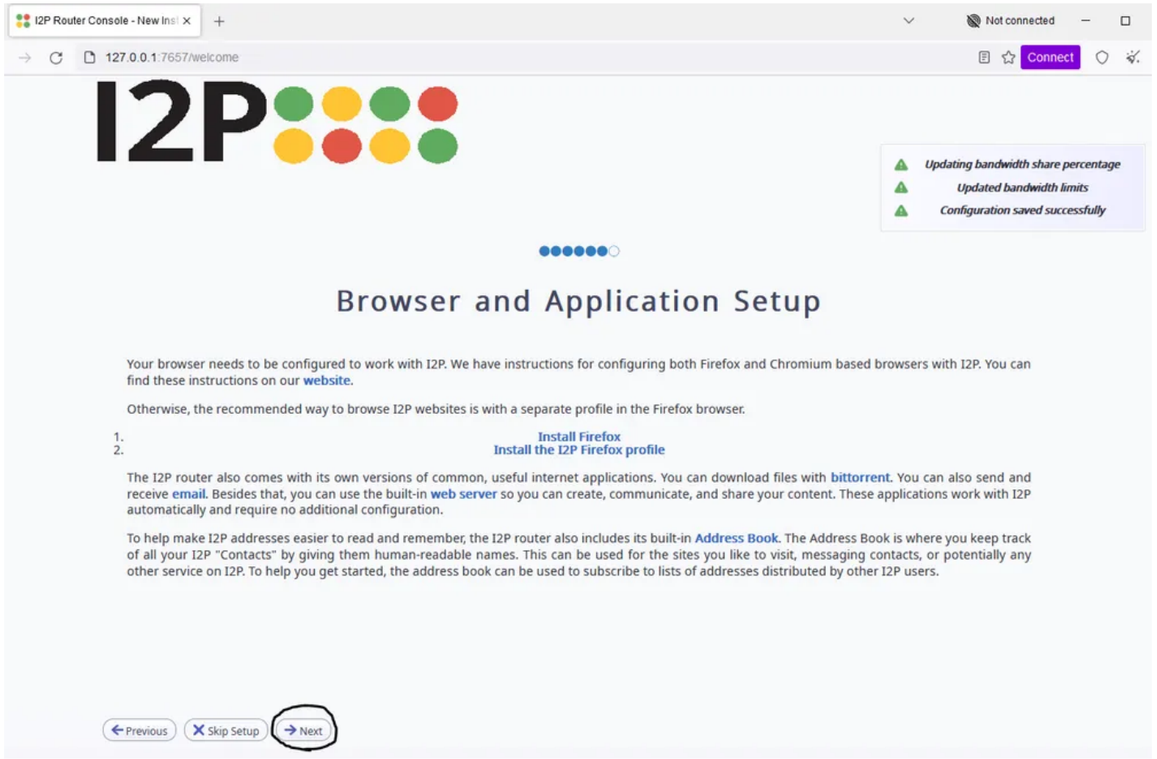


18. Next 클릭.

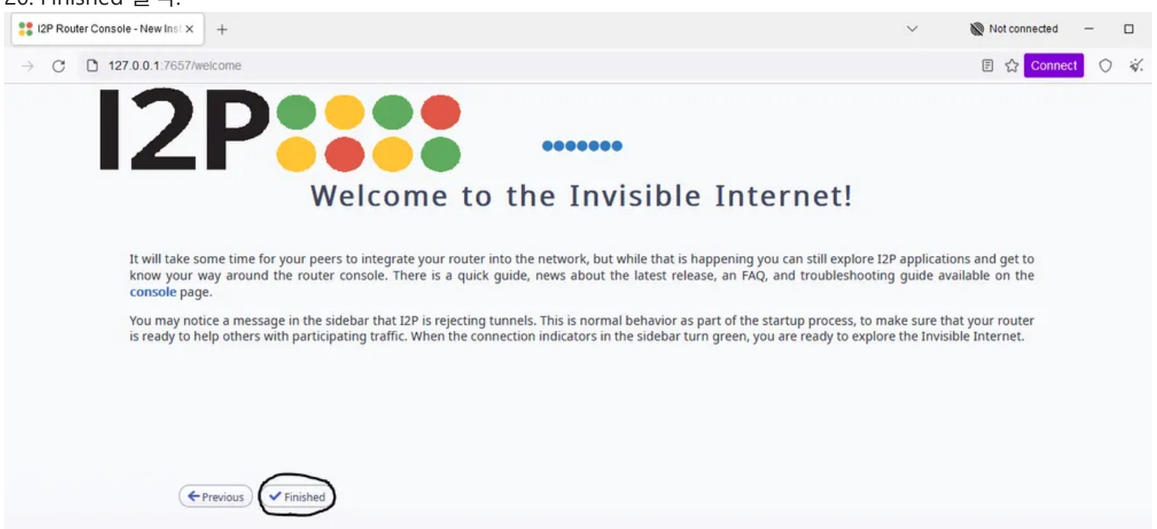


19. Next 클릭.

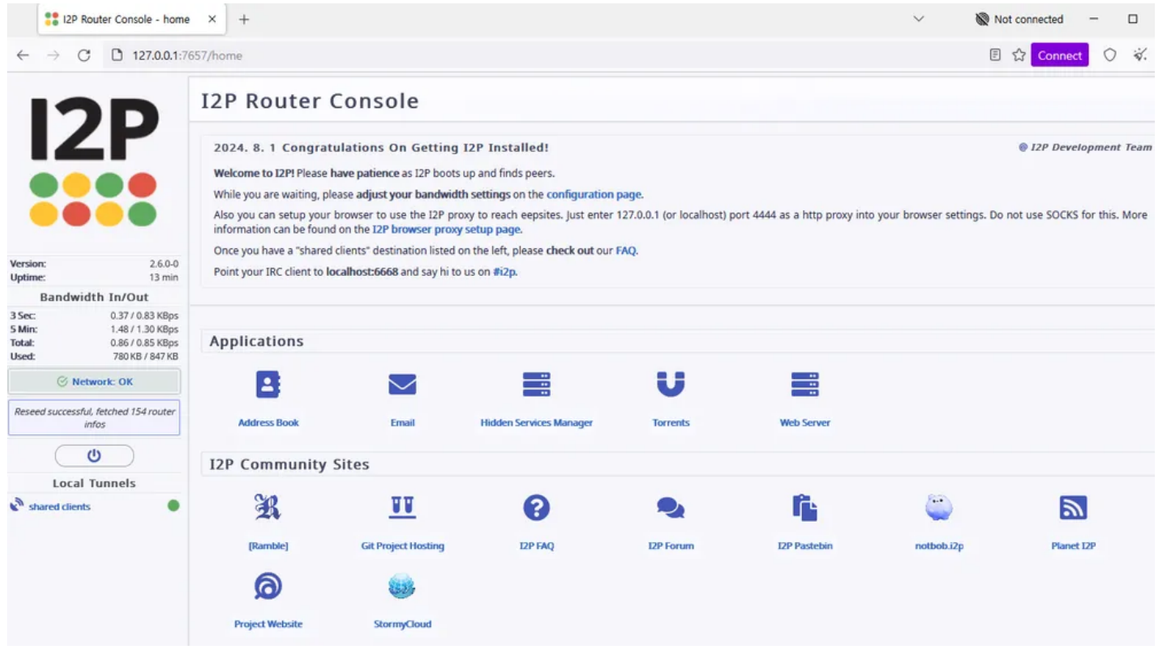




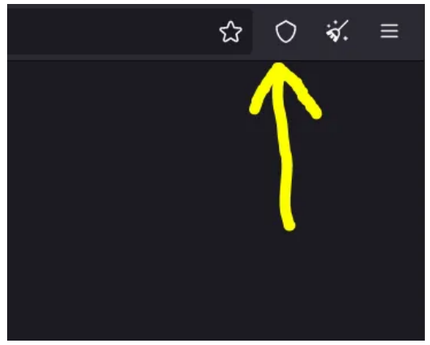
20. Finished 클릭.

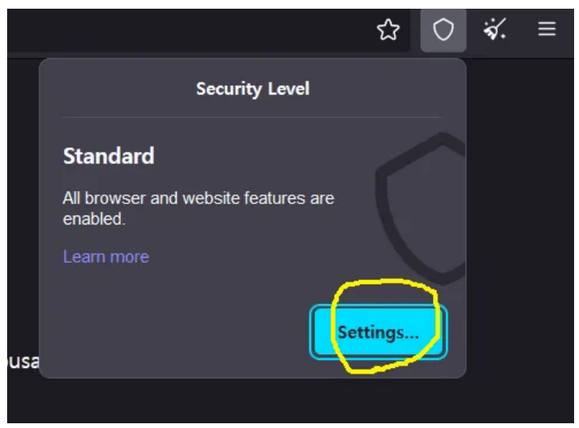


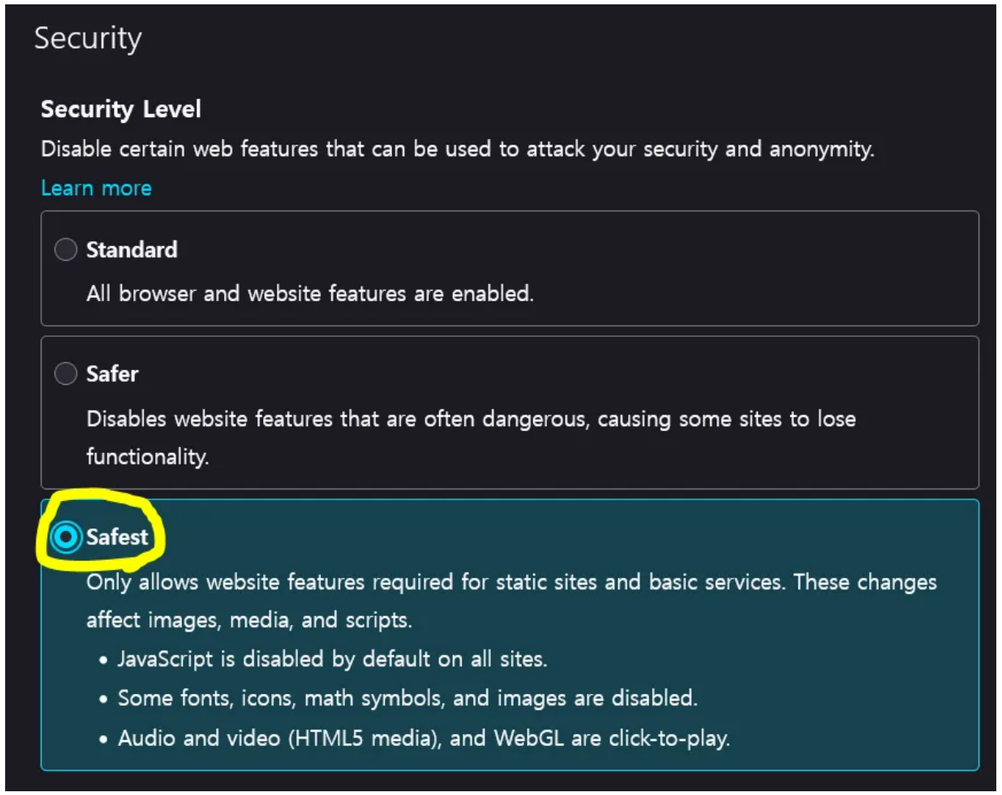
21. 메인 홈페이지의 모습이다.



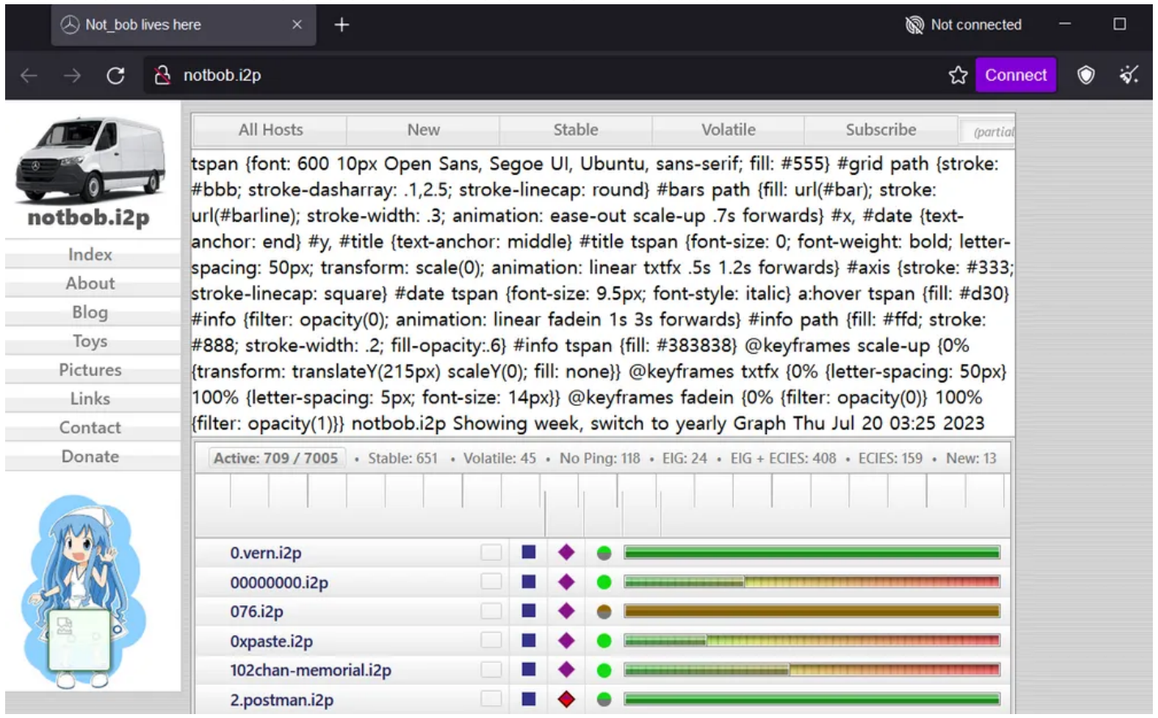
22. 토어 브라우저의 보안 레벨을 Safest로 변경한다.



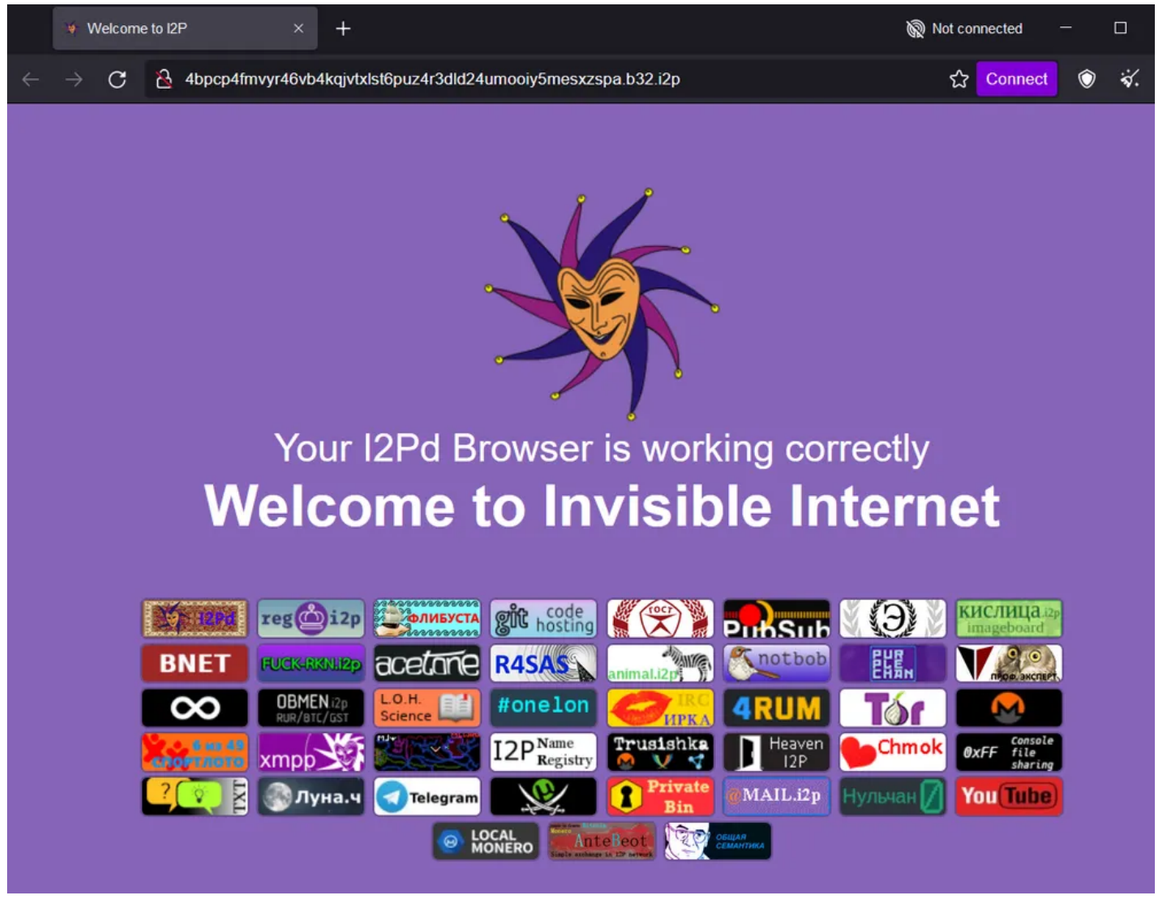


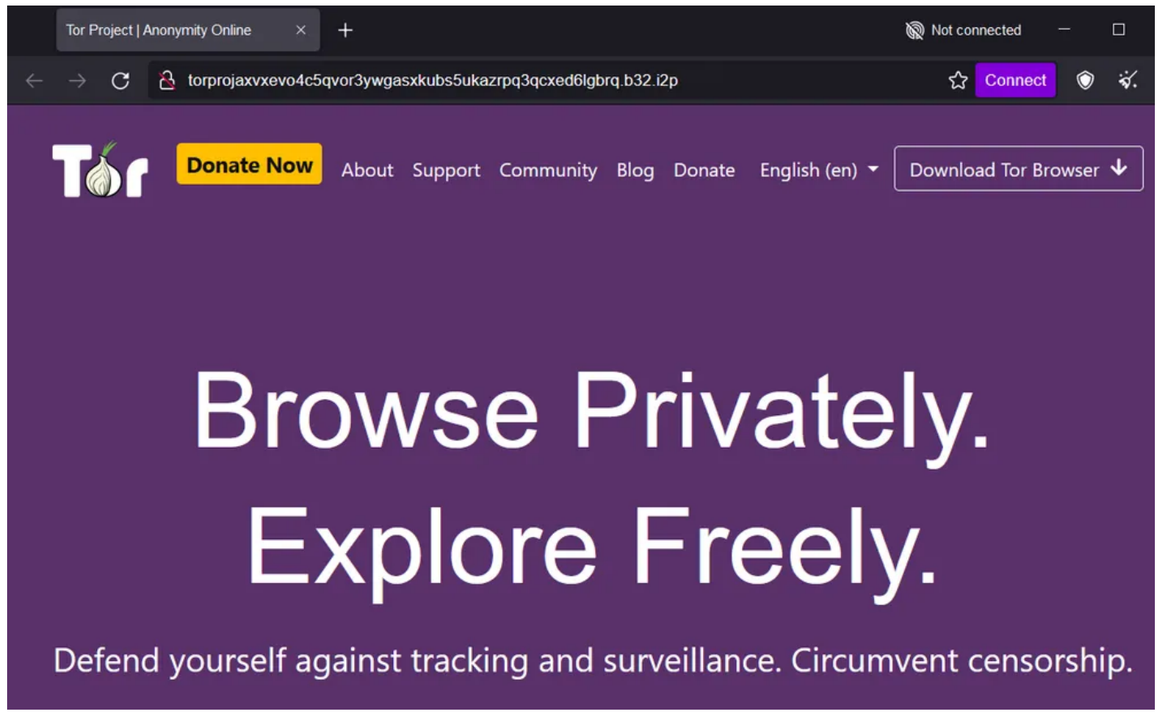


23. notbob.i2p 사이트에 접속했을 때의 모습이다. 사이트가 살짝 깨졌지만 이용에는 큰 지장 없다. 아이콘에 마우스를 갖다 대면 나오는 왼쪽 아래의 주소 문구로 사이트 분류를 알 수 있다.



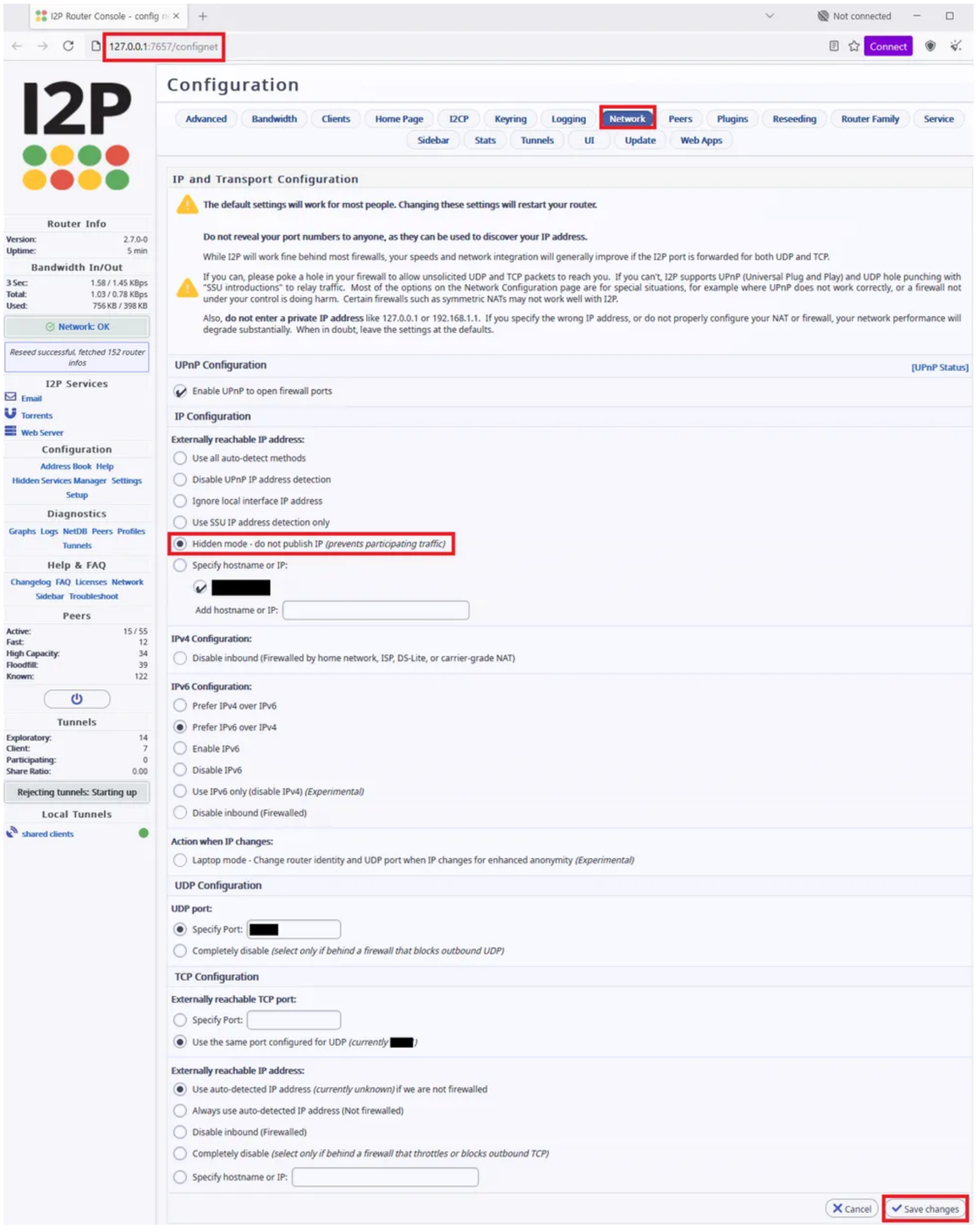
24. 각종 웹사이트를 탐방할 수 있다.

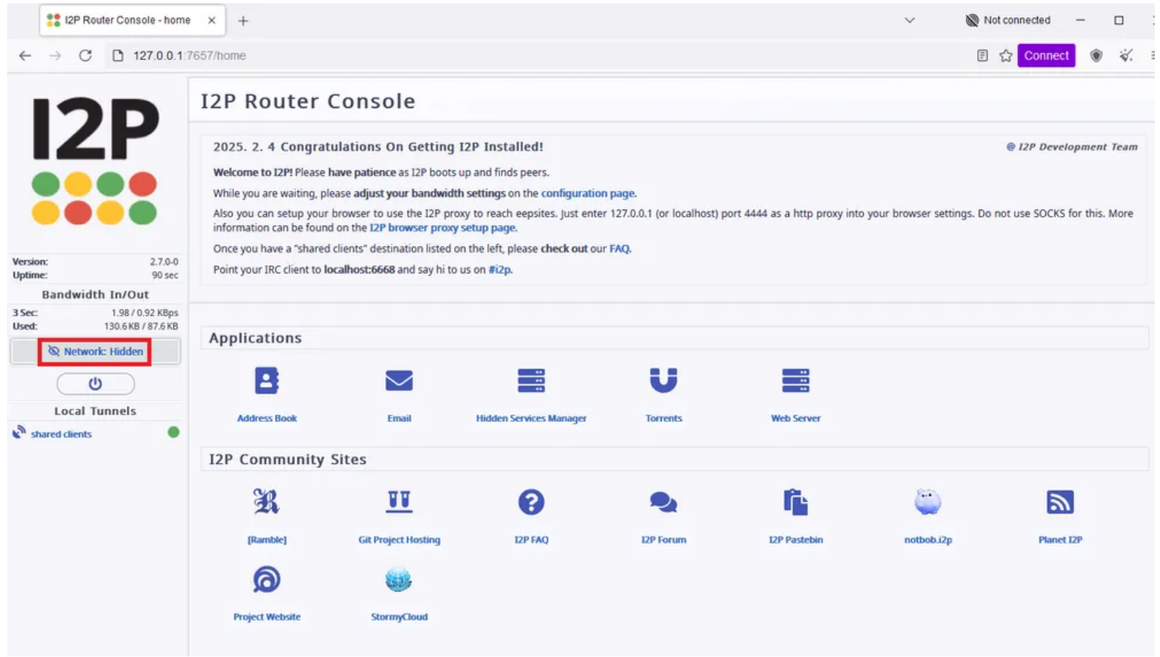




지금까지 토어 브라우저를 세팅하여 I2P를 이용하는 방법을 알아보았다.

4. Hidden Mode





https://geti2p.net/en/about/restrictive-countries

감시가 심한 국가에서는 자동으로 숨김 모드(hidden mode)가 활성화된다. 설정에서 숨김 모드(hidden mode)를 수동으로 활성화할 수 있다.

라우터가 숨김 모드(hidden mode)로 전환되면 세 가지 주요 동작이 변경된다. 더 이상 NetDB에 routerInfo를 게시하지 않고, 참여 터널을 허용하지 않으며, 라우터가 있는 국가에 있는 라우터에 대한 직접 연결을 거부한다.

Tor의 브리지(Bridge)와 비슷한 역할을 한다고 이해하면 된다.

5. I2PSnark

오류가 발생했습니다.

www.youtube.com에서 동영상을 시청하거나 브라우저에서 자바스크립트가 사용 중지된 경우 사용 설정하세요.

오류가 발생했습니다.

www.youtube.com에서 동영상을 시청하거나 브라우저에서 자바스크립트가 사용 중지된 경우 사용 설정하세요.

위 영상의 tracker2.postman.i2p 사이트는 2023년에도 살아있다. ~~살아있는 화석 ㄷㄷ~~

I2PSnark라는 익명 비트토렌트 프로그램이 I2P에 내장되어 있다.

I2PSnark의 본질은 토렌트이고, 토렌트는 다운과 동시에 업로드가 된다는 사실을 꼭 알아둬야 한다. 그리고 I2P을 사용하여 저작권이 있는 자료를 원작자 허가 없이 업로드/다운로드하는 것은 불법 공유이다. 불법 공유는 범죄이므로 하면 안 된다.

6. I2PD

https://i2pd.website/

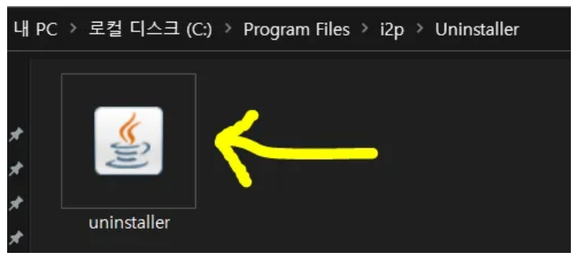
I2PD를 사용하여 I2P를 탐방할 수도 있다.

7. Syndie

자세한 내용은 Syndie 문서를 참고하면 된다.

8. I2P 삭제

I2P 삭제하는법
I2P 삭제하기



I2P를 삭제하려고 제어판 -> '프로그램 및 기능'에 들어갔는데 I2P가 안 보여서 당황할 수도 있다. 이미지의 'uninstaller'를 클릭하여 I2P를 삭제할 수 있다.

9. 모네로

암호화폐 모네로는 I2P를 사용하여 거래자의 IP 주소를 숨길 수 있는 Kovri 프로젝트를 개발 중이다.

Keepit History: 익명화폐의 역사 2편

10. 억압적인 국가에서의 검열 우회

> If I take your question as "What to do if I'm worried about getting caught running an I2P router in an oppressive regime," and you are worried about the authorities associating your computers with I2P traffic in the long term, and you still want to run an I2P router, then there are generally two solutions:
>
> - Run I2P off-site somewhere it is legal, and access it via an innocuous-seeming form of encrypted connection, such as an SSH connection or an HTTPS connection.
> - Encapsulate your I2P traffic in something legal. If a VPN is legal, then that I guess. If SSH is legal, an SSH tunnel.
>
> But, suppose your adversary is waiting for you to download a particular file that they know you are going to try and download anonymously. If they observe you downloading something that looks like a file of a similar size on your HTTPS tunnel or SSH tunnel or VPN, they're just going to assume that file is what they wanted to catch you with and come after you anyway.
> In fact, at the point where your adversary is willing to go after all I2P users, or all Tor users, or all bittorrent users or TLS users or bitcoin users or whatever, it's impossible to just give people "Settings" that can guarantee they will never be under suspicion. I mean, presumably you got an executable installer from https://i2p.net/, right? So you made DNS requests that say "I'm interested in I2P" you connected to the I2P web site and you downloaded a file about ~18.5 Mb in size. In such a draconian regime, you either get I2P from an unofficial channel, likely a sneakernet channel, or you are already under suspicion. Then you have to re-seed from a channel that can't be monitored easily as well, hopefully your sneakernet guy brought you a fresh reseed file to start with. You get the internet you use it on with a cantenna. You get the idea. In these kinds of very oppressive regimes, technology must be combined with planning, including possibly escape plans.
> Fortunately, only a few countries have this kind of law so far.
> 만약 당신의 질문을 "억압적인 정권 아래에서 I2P 라우터를 운영하다가 적발될까 봐 걱정된다면 어떻게 해야 할까요?"로 이해한다면, 그리고 당국이 당신의 컴퓨터를 I2P 트래픽과 장기적으로 연관시킬까 봐 걱정되지만, 그럼에도 불구하고 I2P 라우터를 운영하고 싶다면 일반적으로 두 가지 해결책이 있습니다.
>
> - I2P를 합법적인 외부 장소에서 운영하고, SSH 연결이나 HTTPS 연결처럼 무해해 보이는 암호화된 연결을 통해 접속하는 것입니다.
> - I2P 트래픽을 합법적인 방식으로 캡슐화하는 것입니다. VPN이 합법적이라면 VPN을 사용할 수 있고, SSH가 합법적이라면 SSH 터널을 사용할 수 있습니다.
>
> 하지만, 만약 당신의 적이 당신이 익명으로 다운로드하려는 특정 파일을 기다리고 있다고 가정해 봅시다. 만약 적이 당신이 HTTPS 터널이나 SSH 터널, 또는 VPN을 통해 비슷한 크기의 파일을 다운로드하는 것을 목격한다면, 그들은 그 파일이 당신이 익명으로 다운로드하려던 파일이라고 단정짓고 당신을 추적할 것입니다.
> 사실, 적이 모든 I2P 사용자, 모든 Tor 사용자, 모든 Bittorrent 사용자, TLS 사용자, 모든 Bitcoin 사용자 등을 표적으로 삼으려 한다면, 사람들이 절대 의심받지 않도록 보장하는 "설정"을 제공하는 것은 불가능합니다. 예를 들어, 여러분은 https://i2p.net/에서 실행 가능한 설치 프로그램을 다운로드했을 겁니다. 즉, "I2P에 관심이 있습니다"라는 DNS 요청을 보내고, I2P 웹사이트에 접속해서 약 18.5MB 크기의 파일을 다운로드했을 겁니다. 이렇게 엄격한 규제 체제에서는 비공식 채널, 아마도 Sneakernet 채널을 통해 I2P를 다운로드하거나, 아니면 이미 의심을 받는 상황에 놓이게 됩니다. 게다가 감시가 어려운 채널에서 시드 파일을 다시 제공해야 하는데, Sneakernet에서 제공한 파일이 처음부터 새것이기를 바라야겠죠. 인터넷 연결은 안테나 같은 걸로 합니다. 대충 어떤 상황인지 아

> 시겠죠? 이처럼 억압적인 체제에서는 기술과 함께 탈출 계획을 포함한 철저한 준비가 필수적입니다.
> 다행히 현재까지 이러한 법을 제정한 나라는 극소수에 불과합니다.
>
> https://www.reddit.com/r/i2p/comments/bfh6cd/if_you_live_in_very_hostile_region_of_the_world/ @

> To me, the safest way to run freenet in a hostile country is the following:
>
> - Know Freenet users either in countries with more relaxed laws or people who know people
> - Install freenet in a VM that's using full disk encryption OR on a VPS in another country. If remote node, connect to fproxy via SSH tunnel. Deleting a VM using full disk encryption takes seconds and is hard to recover valuable data from.
> - Connect with friends as darknet peers. Make sure they're not an informant. This is an opsec thing.
> - Use Freenet
>
> Never run your node in anything but high security, even once.
> 제 생각에 적대적인 국가에서 Freenet을 안전하게 운영하는 가장 좋은 방법은 다음과 같습니다.
> - 법이 비교적 완화된 국가의 Freenet 사용자 또는 그들을 아는 사람들을 통해 Freenet 사용자를 확보하세요.
> - 전체 디스크 암호화를 사용하는 가상 머신(VM) 또는 다른 국가의 VPS에 Freenet을 설치하세요. 원격 노드인 경우 SSH 터널을 통해 fproxy에 연결하세요. 전체 디스크 암호화(Full Disk Encryption)를 사용하는 VM은 삭제하는 데 몇 초밖에 걸리지 않으며 중요한 데이터를 복구하기 어렵습니다.
> - 친구들과 Darknet 피어로 연결하세요. 정보원이 아닌지 반드시 확인하세요. 이는 작전 보안과 관련된 사항입니다.
> - Freenet을 사용하세요.
>
> 노드를 실행할 때는 절대로 최고 수준의 보안 설정 외에는 다른 설정을 사용하지 마십시오. 단 한 번이라도 사용해서는 안 됩니다.
>
> https://www.reddit.com/r/Freenet/comments/bfh6oe/if_you_live_in_very_hostile_region_of_the_world/ @

> If you're going to be in a place where you're worried about that, your laptop will be searched on arrival, and fairly well. You will need to go further, and hide the application. Maybe even compile it once you arrive.
> Being caught with these things on your computer upon entrance to said country might land you in prison.
> 만약 그런 문제가 걱정되는 곳에 가신다면, 도착 시 노트북 검사를 꽤 꼼꼼하게 받게 될 겁니다. 더 나아가, 해당 애플리케이션을 숨겨야 할 수도 있습니다. 어쩌면 도착 후에 직접 컴파일해야 할지도 모릅니다.
> 해당 국가 입국 시 컴퓨터에 이런 것들이 있는 것이 적발되면 투옥될 수도 있습니다.
>
> https://www.reddit.com/r/i2p/comments/bfh6cd/if_you_live_in_very_hostile_region_of_the_world/ @

https://www.whonix.org/wiki/Bridges

USER -(SSH)-> VPS -(Tor,I2P,Hyphanet,GNUnet)-> Website

신뢰할 수 있는 VPS에 Tor, **I2P**, Hyphanet, GNUnet 같은 프로그램을 설치하고 SSH로 터널링(Tunnelling)하여 ISP로부터 익명 네트워크 사용을 숨길 수 있다. ISP는 유저가 VPS와 SSH로 통신하고 있다는 사실만 알 수 있다. 단 이용하는 VPS를 신뢰해야 한다는 단점이 있다.

11. 같이 보기

- 인터넷 프라이버시

이 저작물은 CC BY-NC-SA 2.0 KR에 따라 이용할 수 있습니다. (단, 라이선스가 명시된 일부 문서 및 삽화 제외)
기여하신 문서의 저작권은 각 기여자에게 있으며, 각 기여자는 기여하신 부분의 저작권을 갖습니다.

나무위키는 백과사전이 아니며 검증되지 않았거나, 편향적이거나, 잘못된 서술이 있을 수 있습니다.
나무위키는 위키위키입니다. 여러분이 직접 문서를 고칠 수 있으며, 다른 사람의 의견을 원할 경우 직접 토론을 발제할 수 있습니다.